BBN Technologies
10 Moulton Street
Cambridge, MA 02138

6 March 2017

US Navy
Office of Naval Research
One Liberty Center
875 North Randolph Street
Arlington, VA 22203-1995

Delivered via Email to:
richard.t.willis@navy.mil
ravindra.athale@navy.mil
richard.lepkowicz.ctr@navy.mil
alexander.gorelik@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil

Contract Number:	N00014-16-C-2069
Proposal Number:	P15030A-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Saikat Guha
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	COmmunications and Networking with QUantum operationally-Secure Technology for Maritime Deployment (**CONQUEST**)
Contract Period of Performance:	2 September 2016 – 1 September 2019
Total Contract Amount:	$3,663,297
Year 1 Contract Amount:	$1,219,339
Amount of Incremental Funds:	$617,413
Total Amount Expended + Committed Funds (thru 3 March):	$281,780 + $86,643

Attention: Dr. Richard T. Willis
Subject: Quarterly Progress Report
Reference: Section J, Exhibit A: Contract Data Requirements List

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Saikat Guha at 617.873.5122 (email: saikat.guha@raytheon.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kathryn.carson@raytheon.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson

Kathryn Carson
Program Manager
Quantum Information Processing

CONQUEST Quarterly Progress Report #2 for the Period
2 December 2016 – 1 March 2017 (3 Months)

Section A. Task Progress

A program review meeting was held at ONR's meeting site in Arlington, VA on February 16th and 17th with all team members in attendance. See attached slides from review meeting showing team progress against tasks.

Section B. Planned Activities/Schedule

Monthly team meetings have been scheduled and the last monthly meeting was held at MIT on February 13th. The next scheduled team meeting will be held via teleconference on March 9th. BBN's internal team meetings are scheduled for every other Tuesday morning. For information regarding planned technical activities, see the updates provided in the attached slides.

Section C. Equipment Purchased

No equipment has been purchased or constructed at this time.

Section D. Key Personnel

There have been no changes in personnel.

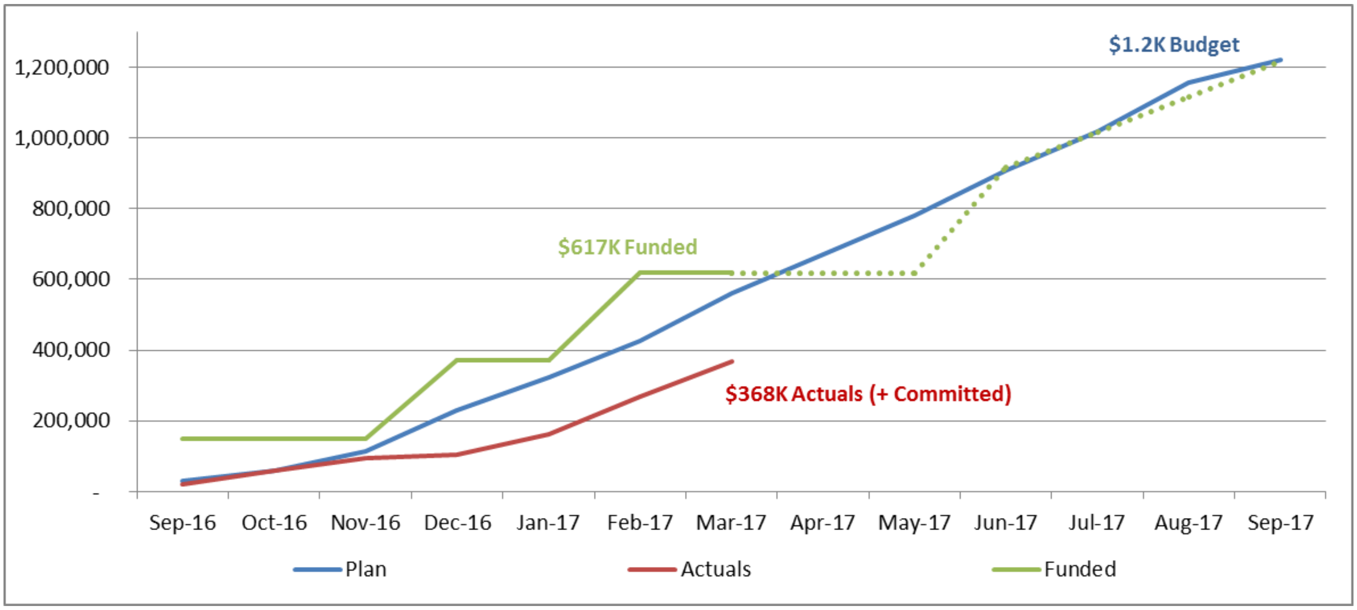
Section E. Accomplishments

See updates provided in Sections A and B above. In addition, please find attached a memo from Jeff Shapiro in response to the SPAWAR-provided atmospheric data.

Section F. Anticipated Problems

There are no anticipated problems or issues to report at this time.

Section G. CONQUEST Budget



Questions Regarding "Quantum Key Distribution: Atmospheric Profiles of Extinction and Turbulence"

Jeffrey H. Shapiro

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

(Dated: February 2, 2017)

Dr. Tommy Willis (Office of Naval Research) has asked his Maritime QKD teams to employ the SPAWAR-provided atmospheric extinction and turbulence data from [1] to assess the operational utility of their respective quantum key distribution (QKD) protocols. The present memo raises a series of questions about that data that are relevant to the Raytheon-BBN led CONQUEST team's attempt to follow through on Dr. Willis' request.

Introduction

Drs. McBryde and Hammel have prepared a compilation of atmospheric extinction and turbulence data for a 30-km-long maritime path [1]. In particular, they have used atmospheric models for absorption, scattering, and refractive-index turbulence as functions of the principal meteorological parameters to generate vertical profiles (from $h = 1$ to $h = 50\,\text{m}$ above the sea surface) of the molecular and aerosol absorption coefficients, the molecular and aerosol scattering coefficients, and the turbulence strength ($C_n^2(h)$) at 780 nm, 1550 nm, and 4000 nm wavelengths. Then, using a huge database of meteorological data from the Point Mugu Sea Range (PMSR), they generated icosile histograms of extinction-only and turbulence-only normalized power-in-bucket (PIB) values when transmission is between equal-height-above-sea-surface terminals that use 26.5-cm-diameter pupils at 19 m, 30 m, or 50 m above the sea surface. Also distributed with Ref. [1] were Excel spreadsheets that provide 10%, 50%, and 90% decile PIB results for extinction-only and turbulence-only conditions at the three wavelengths, along with sample height profiles from each of those deciles of the molecular and aerosol absorption coefficients, the molecular and aerosol scattering coefficients, and $C_n^2(h)$, plus (for the turbulence case) the Fried parameter r_0 for each of these PIB deciles. In the CONQUEST team's attempt to make use of this trove of information a number of questions have arisen. The purpose of this memo goes beyond merely asking those questions. Indeed, it explains how they have arisen in trying to use the data provided in [1].

Transceiver Question

In [2] we learned that Ref. [1] assumes a transmitter exit pupil and a receiver entrance pupil that are 26.5-cm-diameter unobscured circular apertures. For our performance analyses, we plan to assume the transmitter employs a uniform-intensity, focused-beam, spatial mode. In particular, if $E_0(\boldsymbol{\rho})$ and $E_L(\boldsymbol{\rho}')$ are the $\sqrt{\text{W/m}^2}$ complex field envelopes at $\boldsymbol{\rho} = (x, y)$ in the transmitter's exit pupil and $\boldsymbol{\rho}' = (x', y')$ in the receiver's entrance pupil for monochromatic (wavelength λ) transmission through a fixed atmospheric state then

$$E_0(\boldsymbol{\rho}) = \begin{cases} \sqrt{\dfrac{4P_T}{\pi d^2}}\, e^{-ik|\boldsymbol{\rho}|^2/2L}, & \text{for } |\boldsymbol{\rho}| \le d/2, \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

where P_T is the transmitted power, $d = 26.5\,\text{cm}$ is the transmitter pupil's diameter, $L = 30\,\text{km}$ is the path length, and $k = 2\pi/\lambda$ is the wave number at the operating wavelength;

$$\text{PIB}_{\text{ext}} \equiv \frac{1}{P_T}\int_{|\boldsymbol{\rho}'|\le d/2} \mathrm{d}\boldsymbol{\rho}'\, |E_L(\boldsymbol{\rho}')_{\text{ext}}|^2 = \frac{1}{P_T}\int_{|\boldsymbol{\rho}'|\le d/2} \mathrm{d}\boldsymbol{\rho}' \left| \int_{|\boldsymbol{\rho}|\le d/2} \mathrm{d}\boldsymbol{\rho}\, E_0(\boldsymbol{\rho}) \frac{e^{ik|\boldsymbol{\rho}'-\boldsymbol{\rho}|^2/2L}}{i\lambda L} \right|^2 e^{-\bar{\alpha}L}, \tag{2}$$

is the extinction-only PIB with

$$\bar{\alpha} \equiv \frac{1}{L}\int_0^L \mathrm{d}z\, \alpha[h_p(z)] \tag{3}$$

giving the path-averaged extinction coefficient along the path from the transmitter ($z = 0$) to the receiver ($z = L$) in terms of the extinction coefficient's height distribution $\alpha(h)$ and the propagation path's height-above-sea-surface

$h_p(z)$ [3]; and

$$\text{PIB}_{\text{turb}} \equiv \frac{1}{P_T}\int_{|\boldsymbol{\rho}'|\le d/2} \mathrm{d}\boldsymbol{\rho}'\,\left\langle |E_L(\boldsymbol{\rho}')_{\text{turb}}|^2\right\rangle = \frac{1}{P_T}\int_{|\boldsymbol{\rho}'|\le d/2}\mathrm{d}\boldsymbol{\rho}'\,\left\langle\left|\int_{|\boldsymbol{\rho}|\le d/2}\mathrm{d}\boldsymbol{\rho}\,E_0(\boldsymbol{\rho})\frac{e^{ik|\boldsymbol{\rho}'-\boldsymbol{\rho}|^2/2L}}{i\lambda L}e^{\chi(\boldsymbol{\rho}',\boldsymbol{\rho})+i\phi(\boldsymbol{\rho}',\boldsymbol{\rho})}\right|^2\right\rangle, \tag{4}$$

being the turbulence-only PIB, where $\langle\cdot\rangle$ denotes averaging over the turbulence, and $\chi(\boldsymbol{\rho}',\boldsymbol{\rho})$ and $\phi(\boldsymbol{\rho}',\boldsymbol{\rho})$ are the log-amplitude and phase fluctuations seen at $\boldsymbol{\rho}'$ in the receiver pupil that turbulence imposes on a point source transmission from $\boldsymbol{\rho}$ in the transmitter pupil.

It should be clear from the preceding development that both PIB's will depend on the choice made for the transmitter's spatial mode. Reference [1] is silent about its choice of spatial mode. In [2] we learned that Ref. [1] assumed a Gaussian beam,

$$E_0(\boldsymbol{\rho}) = \begin{cases} \dfrac{\sqrt{P_T}\,e^{-|\boldsymbol{\rho}|^2/r^2-ik|\boldsymbol{\rho}|^2/2R}}{\sqrt{\displaystyle\int_{|\boldsymbol{\rho}|\le d/2}\mathrm{d}\boldsymbol{\rho}\,e^{-2|\boldsymbol{\rho}|^2/r^2}}}, & \text{for } |\boldsymbol{\rho}|\le d/2,\\[2ex] 0, & \text{otherwise,}\end{cases} \tag{5}$$

but we were not given values for r and R, although it was tentatively stated that $r = d/2$ and $R = L$. Our transceiver question is therefore as follows.

Transceiver Question: ***What is e^{-2}-attenuation intensity radius, r, and the phase curvature, R, for the Gaussian-beam spatial mode used in Ref. [1]?***

Decile Questions

In studying Ref. [1] and its accompanying spreadsheets, we noted that the memo's icosiles rank the extinction-only and turbulence-only PIBs from low to high, i.e., the 10% icosile's PIB is less than the 50% icosile's PIB that, in turn, is less than the 90% icosile's PIB. The opposite, however, is true for the deciles, viz, the spreadsheets' extinction-only and turbulence-only 10% decile PIBs exceed their 50% counterparts that, in turn, exceed the 90% decile PIBs. Going forward, we will employ the deciles information, because numerical values are provided. In order to make best use of that information, however, the team would like answers to the following questions

Decile Question 1: ***Do the 10%, 50%, and 90% decile PIBs in the spreadsheets represent averages of the PIB values in those deciles?***

Decile Question 2: Presuming the answer to Decile Question 1 is yes, what are the minimum values, maximum values, and standard deviations of the PIBs in the 10%, 50%, and 90% deciles?

(The importance of Decile Question 2—which seeks to understand how much PIB variability there is within the 10%, 50%, and 90% deciles—will become apparent in the next section.)

PIB, $\bar{\alpha}$, and r_0 Questions

Our uniform-intensity, focused-beam, spatial mode leads to the following results for PIB_{ext} and PIB_{turb} [4]. For the extinction-only case we have

$$\text{PIB}_{\text{ext}} = \left\{\frac{8}{\pi}\sqrt{D_f}\int_0^1 d\zeta\,J_1(4\sqrt{D_f}\,\zeta)\left[\cos^{-1}(\zeta)-\zeta\sqrt{1-\zeta^2}\right]\right\}e^{-\bar{\alpha}L}, \tag{6}$$

where

$$D_f = \left(\frac{\pi d^2}{4\lambda L}\right)^2 \tag{7}$$

is the vacuum-propagation Fresnel-number product, $J_1(\cdot)$ is the first-order Bessel function of the first kind, and the term in braces is the PIB for vacuum propagation, which we will denote PIB_{vac}. For the turbulence-only case we find

$$\text{PIB}_{\text{turb}} = \frac{8}{\pi}\sqrt{D_f}\int_0^1 d\zeta\,J_1(4\sqrt{D_f}\,\zeta)\left[\cos^{-1}(\zeta)-\zeta\sqrt{1-\zeta^2}\right]e^{-(3.18\zeta d/r_0)^{5/3}/2}, \tag{8}$$

where we have assumed Kolmogorov-spectrum turbulence with zero inner scale and infinite outer scale, and

$$r_0 \equiv 3.18\left[2.91k^2\int_0^L \mathrm{d}z\, C_n^2[h_p(z)](z/L)^{5/3}\right]^{-3/5}, \tag{9}$$

with $C_n^2[h_p(z)]$ being the turbulence-strength parameter along the path from the transmitter ($z=0$) to the receiver ($z=L$) is the spherical-wave Fried parameter [5].

At this point, some general PIB statements deserve presentation. First, PIB_{vac} obeys the following inequality,

$$\text{PIB}_{\text{vac}} \le \min(1, D_f), \tag{10}$$

regardless of the transmitter's spatial mode. Moreover, for the uniform-intensity, focused-beam spatial mode we have that

$$\text{PIB}_{\text{vac}} \to \begin{cases} 1, & \text{for } D_f \gg 1, \\ D_f, & \text{for } D_f \ll 1, \end{cases} \tag{11}$$

whose cases represent the near-field ($D_f \gg 1$) and far-field ($D_f \ll 1$) power-transfer regimes, respectively. Second, PIB_{turb} has the following behavior for the uniform-intensity, focused-beam spatial mode when $D_f \ll 1$,

$$\text{PIB}_{\text{turb}} \to \begin{cases} D_f, & \text{for } r_0 \gg d, \\ \left(\dfrac{\pi d r_0}{4\lambda L}\right)^2, & \text{for } r_0 \ll d, \end{cases} \tag{12}$$

whose cases represent the diffraction-limited ($r_0 \gg d$) and turbulence-limited ($r_0 \ll d$) far-field power-transfer regimes, respectively.

Because Ref. [1] assumes a Gaussian-beam spatial mode for its transmitter's beam pattern, we have taken an untruncated Gaussian beam, namely

$$E_0(\boldsymbol{\rho}) = \sqrt{\frac{8P_T}{\pi d^2}}\, e^{-4|\boldsymbol{\rho}|^2/d^2 - ik|\boldsymbol{\rho}|^2/2L}, \tag{13}$$

as a simple proxy for obtaining general performance results analogous to those in Eqs. (10)–(12) that should be qualitatively indicative of how Eq. (5) with $r = d/2$ and $R = L$ would perform. For this transmitter beam pattern—and D_f still given by Eq. (7)—PIB_{vac} satisfies

$$\text{PIB}_{\text{vac}} = 4\sqrt{D_f}\int_0^\infty \mathrm{d}\zeta\, e^{-2\zeta^2} J_1(4\sqrt{D_f}\,\zeta), \tag{14}$$

which has near-field and far-field power-transfer regimes obeying

$$\text{PIB}_{\text{vac}} \to \begin{cases} 1, & \text{for } D_f \gg 1, \\ 2D_f, & \text{for } D_f \ll 1, \end{cases} \tag{15}$$

For this transmitter beam pattern—and D_f still given by Eq. (7)—PIB_{turb} satisfies

$$\text{PIB}_{\text{turb}} = 4\sqrt{D_f}\int_0^\infty \mathrm{d}\zeta\, e^{-2\zeta^2} J_1(4\sqrt{D_f}\,\zeta) e^{-(3.18\zeta d/r_0)^{5/3}/2}, \tag{16}$$

which has diffraction-limited and turbulence-limited far-field ($D_f \ll 1$) power-transfer regimes obeying

$$\text{PIB}_{\text{turb}} \to \begin{cases} \text{PIB}_{\text{vac}}, & \text{for } r_0 \gg d, \\ D_f, & \text{for } r_0 \ll d, \end{cases} \tag{17}$$

With the preceding results in hand, we now state some questions.

PIB Question 1 ***At each wavelength the sample height profiles given for the molecular absorption and scattering coefficients, the aerosol absorption and scattering coefficients, and the extinction coefficient are the same for all three deciles and for all three terminal heights. Why is it that the PIB_{ext} values at each wavelength for those deciles and terminal heights can differ by more than an order of magnitude? They should all be the same, unless there is a large amount of PIB_{ext} variability within each decile.***

PIB Question 2: ***At some wavelengths the $C_n^2(h)$ profiles are the <u>same</u> for the same decile and different terminal heights. Why is it that the PIB$_{\rm turb}$ values for those cases differ appreciably? They should be the same, unless there is appreciable PIB$_{\rm turb}$ variability within those deciles.***

$\bar{\alpha}$ **Question:** ***For each decile at each wavelength/height choice, how much variability is there in the path-averaged extinction coefficient?***

r_0 **Question 1:** ***Are the reported r_0 values those for the spherical-wave Fried parameter, or those for the plane-wave Fried parameter, $r_0 = 3.18\left[2.91k^2\int_0^L \mathrm{d}z\, C_n^2[h_p(z)]\right]^{-3/5}$? Note that the plane-wave Fried parameter is always greater than its spherical-wave counterpart.***

As the preceding questions clearly suggest, there must be significant—in some cases dramatic—variations of extinction and $C_n^2(h)$ profiles within each of the spreadsheets' deciles. Further evidence for the variability within each wavelength's turbulence-only 90% decile comes from evaluating PIB$_{\rm turb}$ for the 90% decile r_0 values given in the spreadsheets under the assumption that the spreadsheet is reporting the spherical-wave r_0 and using the PIB$_{\rm turb}$ formulas from Eqs. (8) or (16). Such evaluations all give PIB$_{\rm turb}$ values *much* higher than the spreadsheet's PIB$_{\rm turb}$ values. Note that PIB$_{\rm turb}$ is a monotonically increasing function of r_0. So, if the spreadsheet's r_0 values are plane-wave results, then the evidence for high variability in the 90% decile results is even stronger. Of course, Ref. [1]'s use of a truncated Gaussian spatial mode at the transmitter will likely reduce the PIB$_{\rm turb}$ values from those obtained under the assumption of a uniform-intensity focused beam, but if $r = d/2$ and $R = L$, as [2] suggested, it is still true that the spreadsheets' r_0 values will not predict their 90% decile PIB$_{\rm turb}$ values.

An altogether different problem shows up in the 10% PIB$_{\rm turb}$ values given in the spreadsheets for 4000 nm wavelength at 19 m and 50 m heights. The vacuum-propagation Fresnel-number product for 4000 nm wavelength, 30 km path length, and 26.5 cm diameter unobscured circular apertures is $D_f = 0.211$. Yet the 10% decile PIB$_{\rm turb}$ values reported for 19 m and 50 m heights are 0.379 and 0.372, respectively, clearly violating the PIB$_{\rm turb} \le \min(1, D_f)$ upper bound. This leads to our final PIB question.

PIB Question 3: ***How can the 10% decile PIB$_{\rm turb}$ values for 4000 nm wavelength, 30 km path length, and 26.5 cm diameter unobscured circular apertures exceed the $\min(1, D_f)$ upper bound?***

PIBs for Extinction and Turbulence

QKD systems in the maritime environment will suffer transmission losses from both extinction and turbulence. One might argue that the worst scattering—say from a dense fog—occurs in stable air, thus reducing its atmospheric turbulence. Hence combining the worst-case (90% decile) extinction transmissivity with the worst-case turbulence transmissivity to get an overall transmissivity is probably unduly conservative. Likewise combining the best-case (10% decile) extinction transmissivity with the best case turbulence loss to get an overall transmissivity is probably unduly optimistic. Both situations are almost certainly exacerbated by the evidence for significant PIB$_{\rm ext}$ and PIB$_{\rm turb}$ variability within all the deciles. This consideration leads to our final questions.

Extinction and Turbulence Question 1: ***Can you provide information about the correlation (or anti-correlation) between extinction-only transmissivity and turbulence-only transmissivity, e.g., can you provide (at each wavelength) 10%, 50%, and 90% decile PIBs for extinction plus turbulence?***

---

[1] K. McBryde and S. Hammel, "Quantum key distribution: Atmospheric profiles of extinction and turbulence," SPAWAR Systems Center, Pacific.

[2] 26 January 2017 telephone conversation between Dr. Kevin McBryde (SPAWAR), Dr. Boulat Bash (Raytheon BBN), and Prof. Jeffrey Shapiro (MIT).

[3] The height-above-sea-surface, $h_p(z)$, is given by $h_p(z) = \sqrt{[R_e + h_p(L/2)]^2 + (z - L/2)^2} - R_e$, where $R_e = 6.378\times 10^6$ m is the Earth's radius, and $h_p(L/2)$, the propagation path's minimum height-above-sea-surface, can be found from $h_p(L/2) = \sqrt{(R_e + h)^2 - (L/2)^2} - R_e$, with h being the terminals' height-above-sea-surface.

[4] J. H. Shapiro, "Normal-mode approach to wave propagation in the turbulent atmosphere," Appl. Opt. **13,** 2614–2619 (1974).

[5] In our calculations we use $r_0 = 3.18\left[2.91k^2\int_0^{L/2}\mathrm{d}z\, C_n^2[h_p(z - L/2)]\left((z/L + 1/2)^{5/3} + (1/2 - z/L)^{5/3}\right)\right]^{-3/5}$ for the spherical-wave case, and $r_0 = 3.18\left[5.82k^2\int_0^{L/2}\mathrm{d}z\, C_n^2[h_p(z - L/2)]\right]^{-3/5}$ for the plane-wave case.

Distribution Statement A. Approved for Public Release

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Program overview

Saikat Guha

BBN Technologies

ONR QKD Review Meeting
February 17, 2017

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

CONQUEST team

- BBN
  - **Saikat Guha (PI)**, **Boulat Bash**, **Hari Krovi**, **Prithwish Basu**, **Zachary Dutton**, **Jonathan Habif**: QIT, quantum security, secure and covert communications, quantum repeaters, network design and routing
  - **Kathryn Carson**: Program manager
- LSU
  - **Mark Wilde**: QIT, finite-length security analysis
- MIT
  - **Jeff Shapiro, Franco Wong, Dirk Englund, Zheshen Zhang [students: Darius Bunandar, Mihir Pant]**: Quantum optics, FL QKD, PIC for QKD transceivers, theory of non-classical sources and atmospheric propagation modeling
- U. Toronto / CipherQ
  - **Christian Weedbrook, Kamil Bradler**: CV QKD theory and hardware, FPGA, classical post-processing for CV QKD, CV-MDI QKD, repeater analysis

Program Information

• **Contract Name:**	Communications and Networking with Quantum operationally-secure technology for maritime deployment (CONQUEST)
• **Prime Contract Number:**	N00014-16-C-2069
• **BBN Ref ID:**	14660
• **Customer:**	US Navy/ONR
• **Period of Performance:**	**9/2/2016-9/1/2019**

Program Deliverables

	Deliverable	Due Date
1	Quarterly Progress Reports (technical and financial)	**12/1; 3/1; 6/1; 9/1**
2	Program Review Presentation Material	**As required**
3	YR 3 Contractor Manpower Report (all labor hours)	**Annually; by 10/31**
4	Annual Report	**9/1/17; 9/1/18; 9/1/19**
5	List of Property Acquired or Provided	**Annually; by 6/30**
6	Final Report/Design Recommendation Manual	**By 10/2/2019**

Contact Information

Saikat Guha
Principal Investigator
BBN Technologies
saikat.guha@raytheon.com
617-873-5122

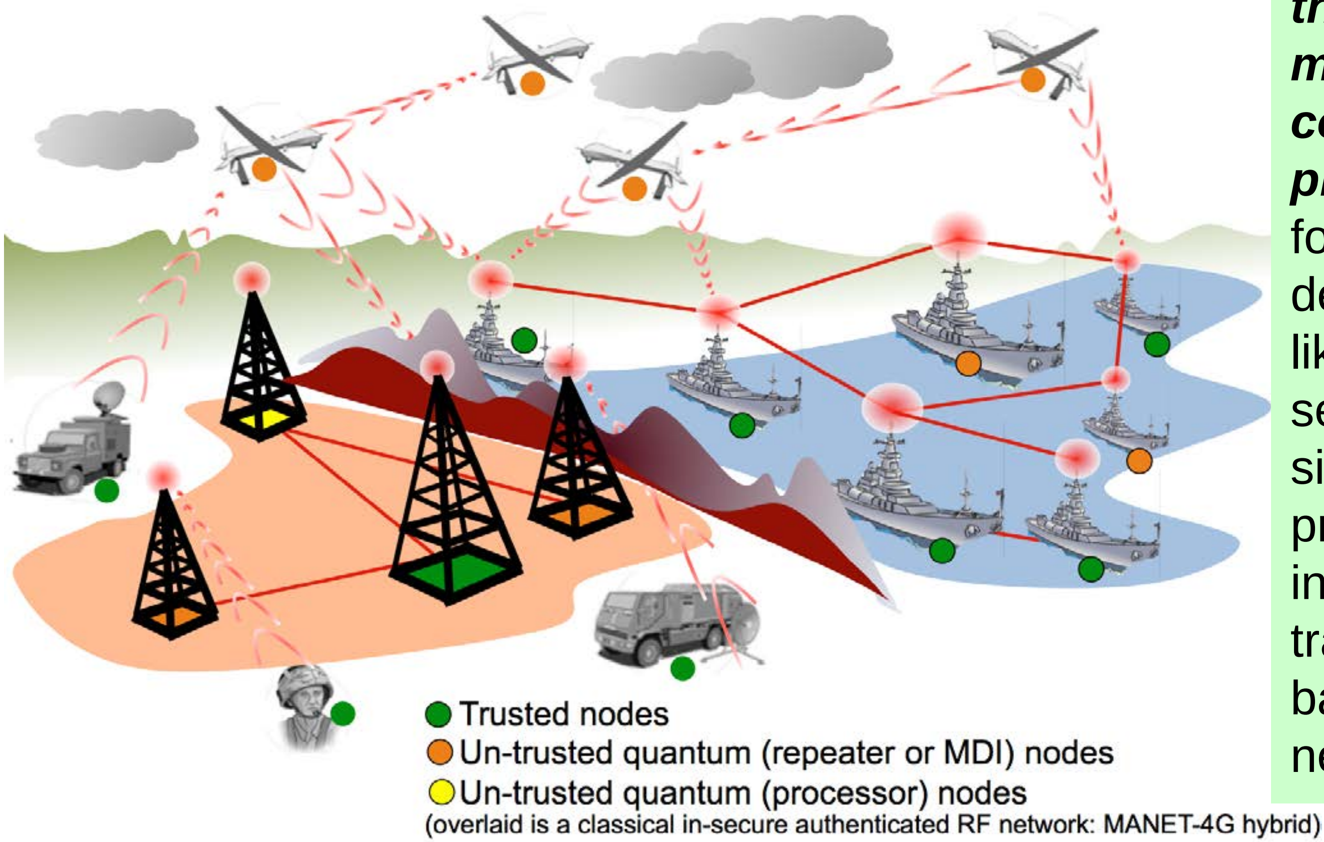
Kathryn Carson
Program Manager
BBN Technologies
kathryn.carson@raytheon.com
617-873-8144

Invoices:
http://connect.transcepta.com/raytheon

CONQUEST program objective

- Quantum-secured free-space optical communications and networking

Goal: advancing the theory and practice of FS QKD over maritime channel conditions with an objective of ***maximizing throughput, and minimizing classical communications and processing overhead*****.** We focus on protocol development (CV and CV-like, discrete constellation), security analyses, finite-size, efficient post-processing, compact integrated-photonic transceiver design, FPGA based post-processing, networking.



Program structure

- Task 1: QKD operation and security analysis for a naval atmospheric link with a realistic eavesdropper
- Task 2: Maritime-implementable QKD protocols
- Task 3: Maximizing the information efficiency of QKD
- Task 4: Improved hardware-domain signal processing
- Task 5: QKD network via un-trusted quantum nodes
- Task 6: Important technical issues to address current deficiencies in the theory/practice of QKD

Saikat / Kathryn - team introduction, task descriptions and technical plan: **10 minutes**

Jeff - Security analysis with realistic eavesdropping assumptions: **15 minutes**

Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**

Kamil - security proof for discrete modulation CV QKD: **15 minutes**

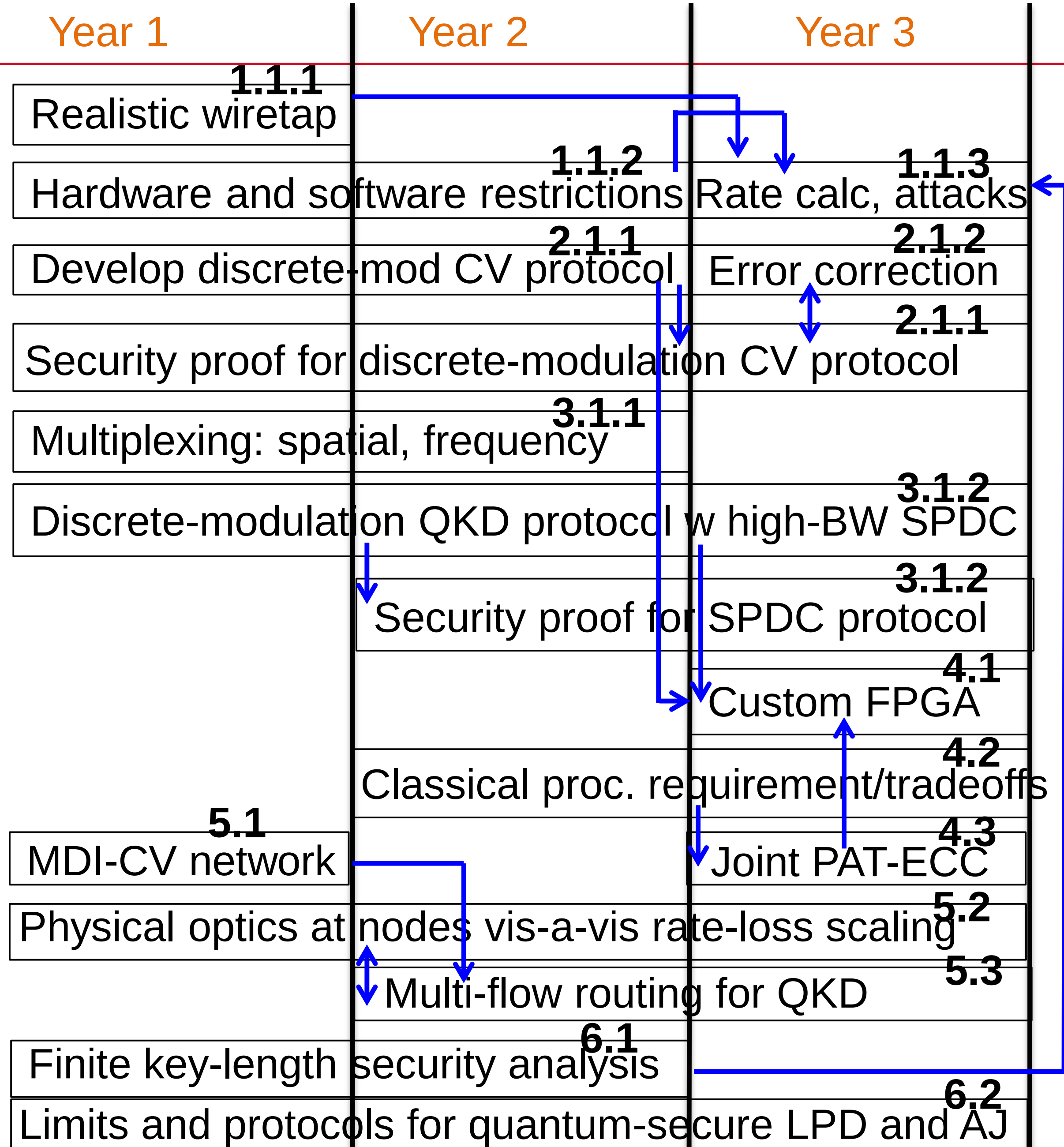
Saikat - efficient post-processing for CV QKD: **15 minutes**

Mark - Finite key-length analysis for QKD: **15 minutes**

Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**

Saikat - Free-space quantum networking / wrap up - **15 minutes**

Task/topic dependencies



Papers in progress and Memos

- M. Takeoka, M. Wilde, “Optimal estimation and discrimination of excess noise in thermal and amplifier channels”, arXiv:1611.09165 (2016).
- B. A. Bash, N. Chandrasekaran, J. H. Shapiro, S. Guha, “Quantum Key Distribution Using Multiple Gaussian Focused Beams,” arXiv:1604.08582 [quant-ph] (2017).
- M. Pant, S. Muralidharan, D. Englund, L. Jiang, and S. Guha, “Resource-cost vs. rate-distance tradeoffs for all-photonic implementation of one-way quantum repeater architecture”, in preparation (2017).
- S. Guha, M. Takeoka, N. Lutkenhaus, “CV QKD with block post-processing”, in preparation (2017).
- M. Takeoka, S. Guha, H. Krovi, N. Lutkenhaus, “Discrete modulation CV QKD with finite-bin post-processing”, in preparation (2017)
- M. Pant, L. Jiang, D. Towsley, P. Basu, H. Krovi, D. Englund, S. Guha, “Multipath routing in a quantum repeater network”, in preparation (2017).
- J. H. Shapiro, “Questions Regarding *Quantum Key Distribution: Atmospheric Profiles of Extinction and Turbulence*, Feb 2, (2017).

Awards

- Prof. Dirk Englund
  - 2017 Adolph Lomb Medal
  - Citation: for pioneering contributions to scalable solid-state quantum memories in nitrogen-vacancy diamond, high-dimensional quantum key distribution, and photonic integrated circuits for quantum communication and computation.
- Dr. Boulat Bash and team
  - 2016 NSA Annual Best Scientific Cybersecurity Paper
  - 2016 Raytheon Excellence in Engineering and Technology (EiET) Award

Quantum-Secure Covert Communication on Bosonic Channels, Boulat Bash, Andrei H. Gheorghe, Monika Patel, Jonathan L. Habif, Dennis Goeckel, Don Towsley, and Saikat Guha, Nature Communications **6**, 8626 (2015)

  - Citation [NSA]: This research adds critical information to the exploration of *covert communications*, the transmission of information without detection by watchful adversaries.

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Eavesdropper Assumptions and Security Requirements: Implications for Secret-Key Rates

Jeffrey H. Shapiro
Massachusetts Institute of Technology

Maritime QKD Review Meeting
February 17, 2017

Raytheon BBN Technologies

LSU LOUISIANA STATE UNIVERSITY

rle RESEARCH LABORATORY OF ELECTRONICS AT MIT

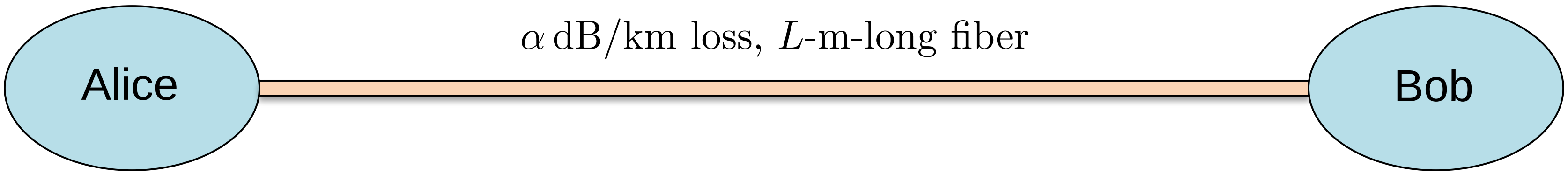
CIPHERQ

Eavesdropper Assumptions and Security Requirements

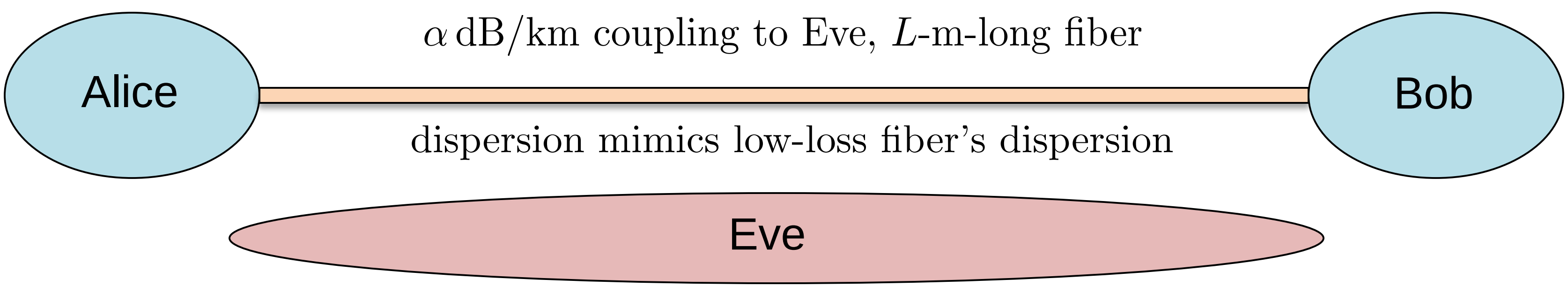
- Attacks on fiber-channel QKD systems
  - undetectable passive eavesdropper
  - coherent, collective, and individual attacks
  - photon-number splitting attack
  - side-channel attacks: blinding and time-shift…
- Attacks on free-space QKD systems
  - passive eavesdropper
  - coherent, collective, and individual attacks
  - realistic attacks on QKD protocol
  - side-channel attacks on QKD equipment

Fiber-Channel QKD: Undetectable Passive Eavesdropper

- Alice and Bob linked by low-loss optical fiber
  - long distance, high loss, no eavesdropper



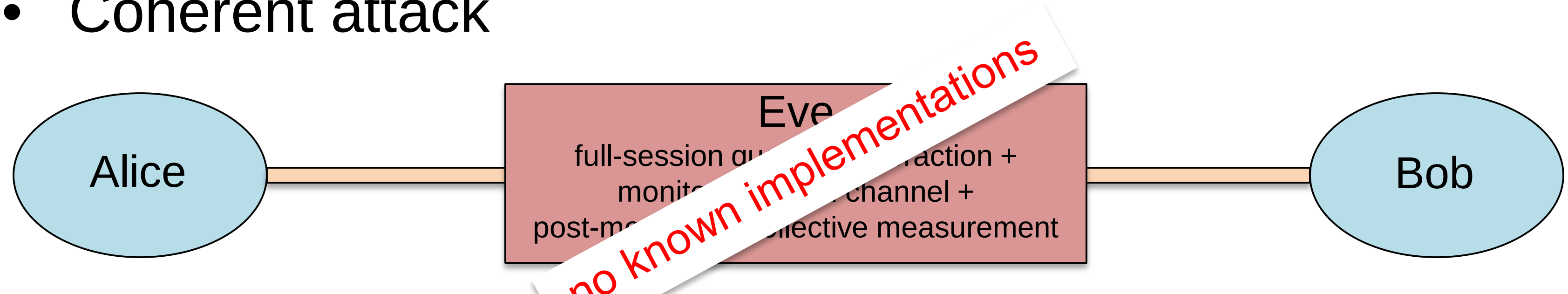
- Attack by undetectable passive eavesdropper
  - long distance, high loss create vulnerability
  - BB84 & CV-QKD security requires low photons/symbol



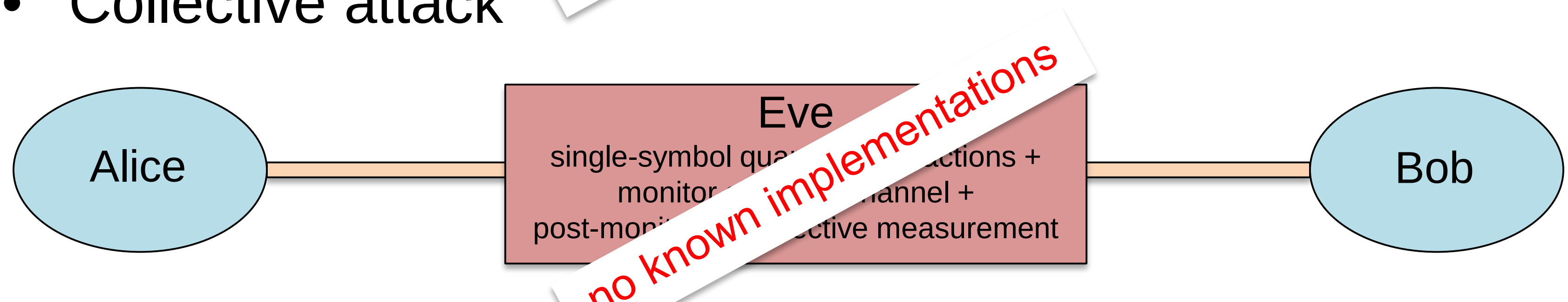
- Long-distance, fiber-channel QKD has low secret-key rate

Fiber-Channel QKD: Coherent, Collective and Individual Attacks

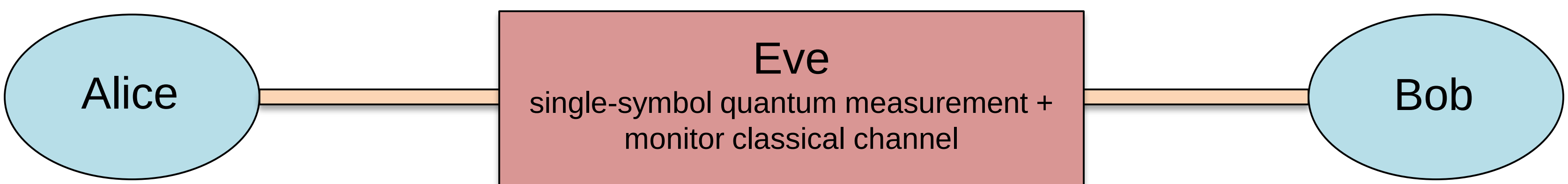
- Coherent attack



- Collective attack

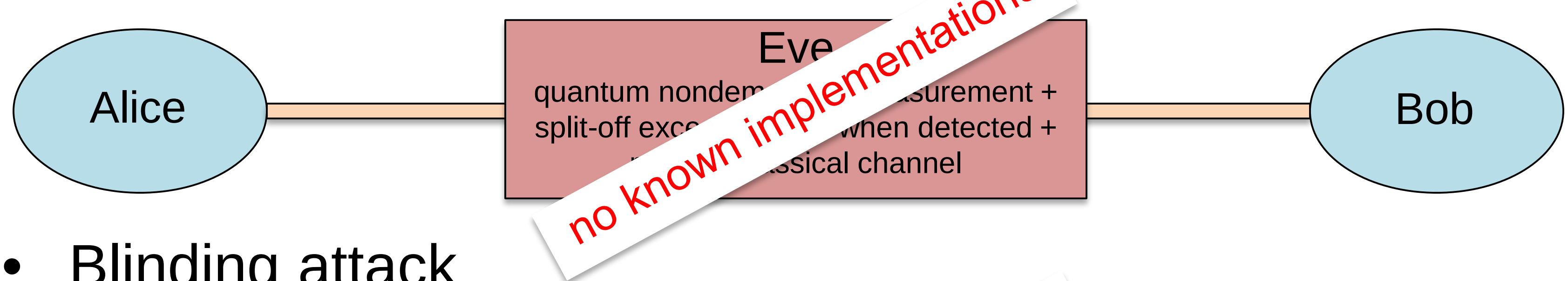


- Individual attack

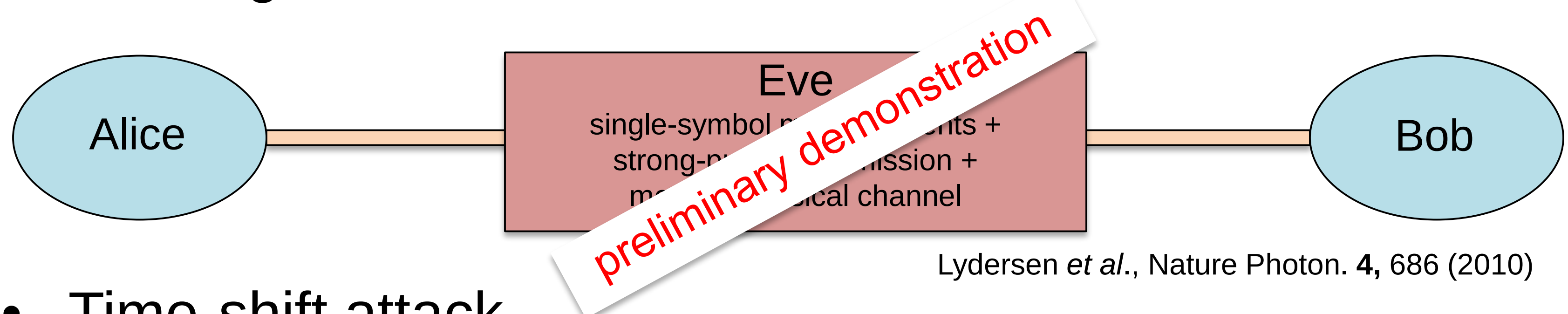


Attacks on Fiber-Channel BB84

- Photon-number splitting attack

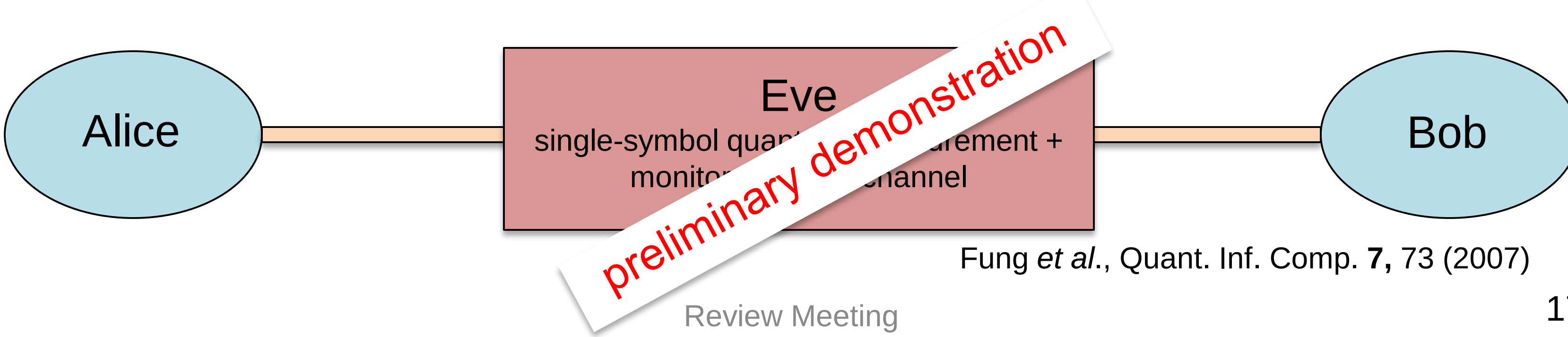


- Blinding attack



Lydersen *et al*., Nature Photon. **4,** 686 (2010)

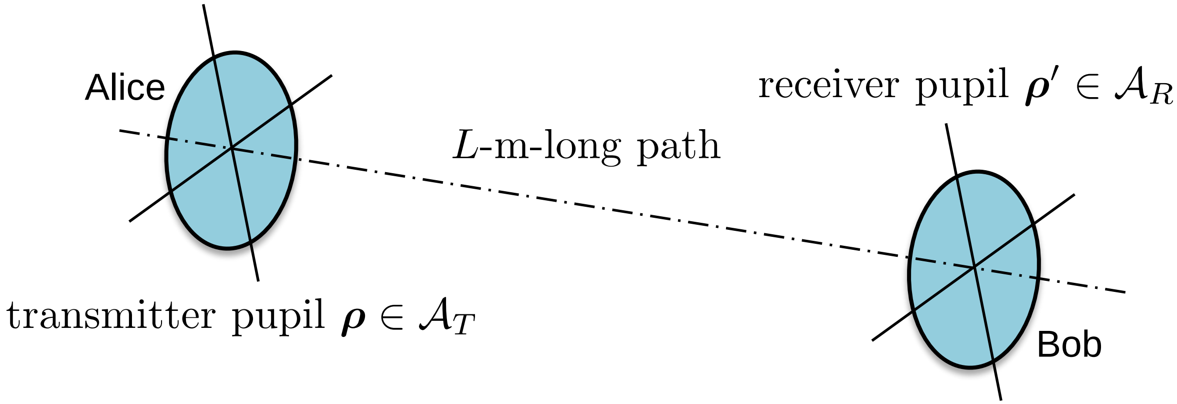
- Time-shift attack



Fung *et al*., Quant. Inf. Comp. **7,** 73 (2007)

Free-Space QKD: Atmospheric Propagation Effects

- Propagation geometry



- Propagation effects
  - absorption
  - depolarization
  - beam spread and angle-of-arrival spread
  - multipath spread and Doppler spread
  - time-dependent fading (scintillation)

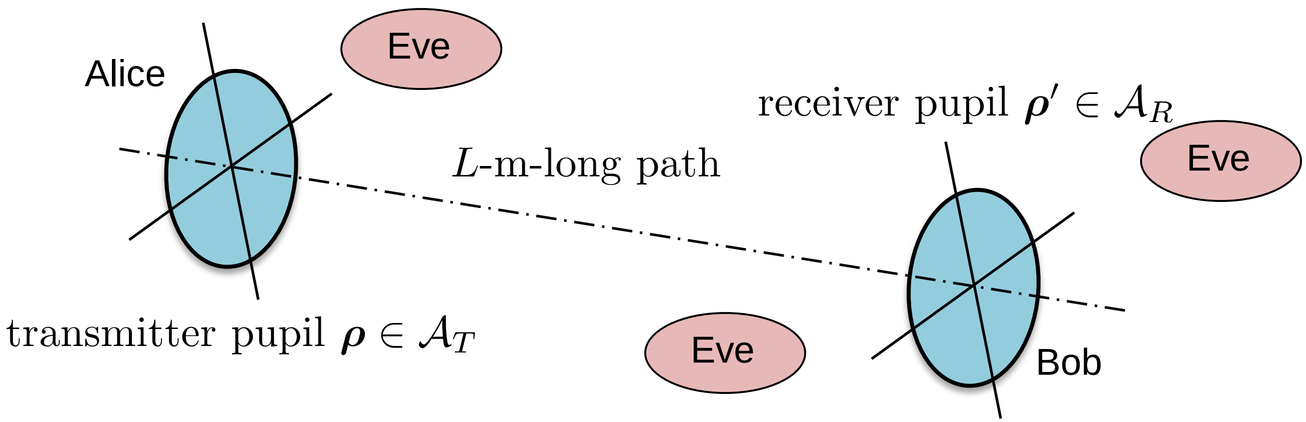
Free-Space QKD: Attacking the Direct-Path Line of Sight

- Eve flies electromagnetically-cloaked drone in direct-path line of sight

  - coherent attack: drone does full-session quantum interaction, monitors classical channel, and does post-monitoring collective measurement
  - backing off to collective attack does not greatly increase feasibility; even individual attack strains credulity

Free-Space QKD: Attacking from Outside the Direct Path

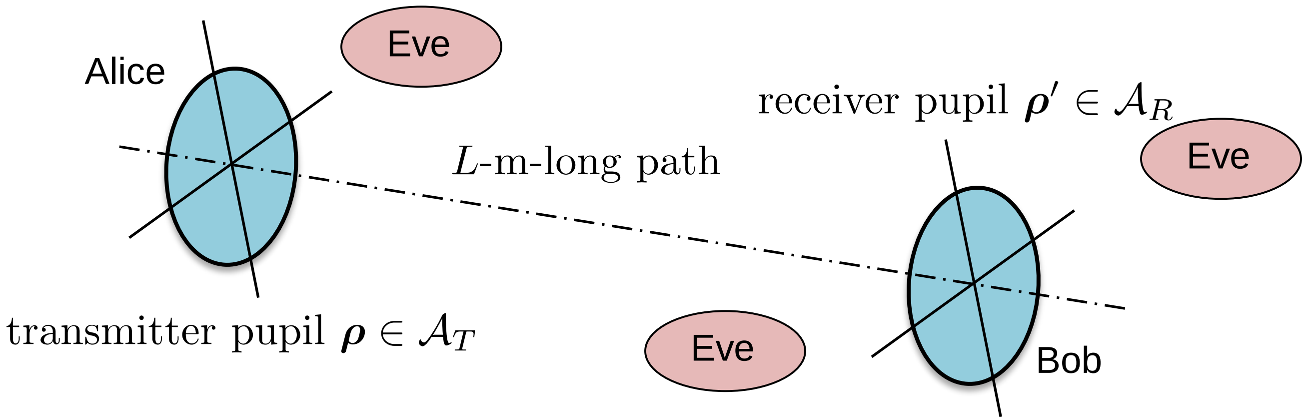
- Eve flies one or more terminals for reception and/or transmission



  - Alice and Bob's line-of-sight observations limit Eve's reception capability — to be determined in Task 1
  - Alice and Bob's field-of-view control limits Eve's transmission capability — to be determined in Task 1

Free-Space QKD: Attacking from Outside the Direct Path

- Eve flies one or more terminals for reception and/or transmission



- Task 1 constraints on Eve's equipment
  - collective attack with finite coherence-time quantum memory
  - individual attack with quantum-limited conventional receiver
- Task 1 options to reduce Eve's capability
  - exploit atmospheric reciprocity with variable-rate transmission
  - exploit atmospheric reciprocity with bidirectional adaptive optics

Eavesdropper Assumptions and Security Requirements

- CONQUEST team will assume that Eve…
  - attacks from outside the line of sight
  - could have a finite coherence-time quantum memory
  - has ideal lasers, squeezers, filters, beam splitters, and single-photon detectors
- CONQUEST team will evaluate…
  - Eve's ability to collect light from the quantum channel
  - Eve's ability to transmit light into Alice and/or Bob
  - Alice and Bob's secret-key rates for principal QKD protocols of interest, e.g., BB84, CVQKD, FL-QKD,…, when operating against Eve's constrained attacks

Preliminary Results: Decoy-State BB84 Secret-Key Rates

- Lower bounds on ergodic secret-key rates (SKRs)

		780 nm wavelength		1550 nm wavelength		4000 nm wavelength	
height	decile	ds-BB84 SKR	Pirandola bound	ds-BB84 SKR	Pirandola bound	ds-BB84 SKR	Pirandola bound
19 m	10%	25.33 Mbps	106.79 Mbps	35.54 Mbps	150.95 Mbps	7.69 Mbps	33.29 Mbps
19 m	50%	0.833 Mbps	5.17 Mbps	1.69 Mbps	8.80 Mbps	0.710 Mbps	4.64 Mbps
19 m	90%	0	35.62 kbps	0	75.21 kbps	0	0.117 Mbps
30 m	10%	95.96 Mbps	443.66 Mbps	108.18 Mbps	510.76 Mbps	13.48 Mbps	57.07 Mbps
30 m	50%	9.06 Mbps	38.93 Mbps	14.44 Mbps	61.05 Mbps	2.89 Mbps	21.88 Mbps
30 m	90%	0	0.492 Mbps	0	1.02 Mbps	13.20 kbps	1.45 Mbps
50 m	10%	159.33 Mbps	831.45 Mbps	162.29 Mbps	852.43 Mbps	15.93 Mbps	67.22 Mbps
50 m	50%	27.65 Mbps	116.70 Mbps	38.33 Mbps	163.23 Mbps	8.76 Mbps	37.70 Mbps
50 m	90%	31.42 kbps	1.54 Mbps	0.336 Mbps	3.14 Mbps	0.560 Mbps	4.00 Mbps

  - average transmissivities: McBryde & Hammel extinction + turbulence profiles and a constant-intensity focused beam
  - DS-BB84 SKR lower bound: Chandrasekaran Ph.D. thesis (MIT EECS, 2016) with 1 Gbps source, unity quantum efficiencies, and 10^{-4} background + dark counts per bit

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Floodlight Quantum Key Distribution: Theory, Experiment, and the Path Forward

Jeffrey H. Shapiro and
Franco N. C. Wong
Massachusetts Institute of Technology

Maritime QKD Review Meeting
February 17, 2017

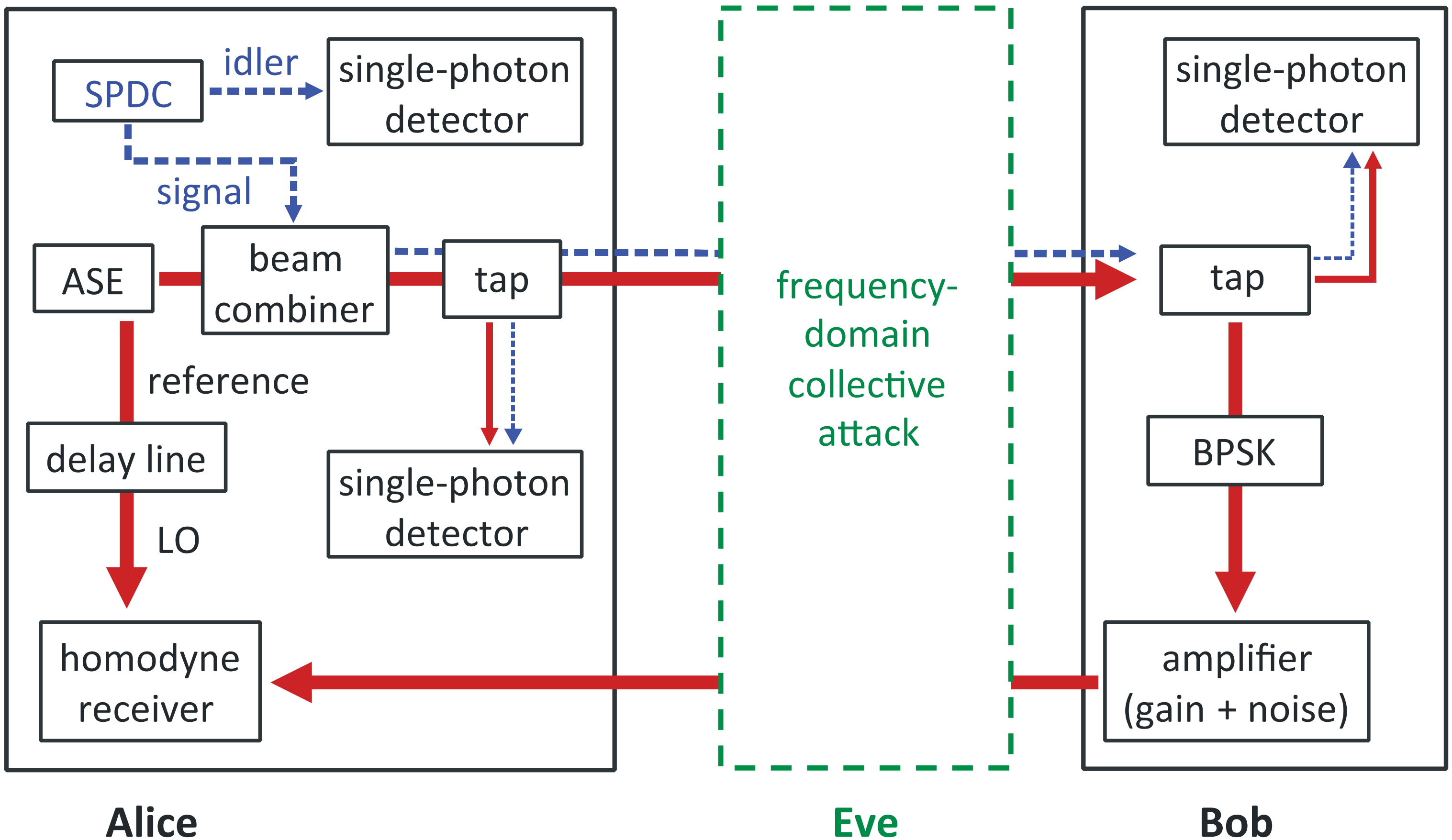
Floodlight Quantum Key Distribution

- FL-QKD protocol
  - low-brightness, broadband source for key generation
  - photon-pair source for security check
- Security analysis and secret-key rates
  - security against optimum frequency-domain collective attack
- Discussion
  - secret-key efficiency: FL-QKD vs. state-of-the-art systems
- Preliminary experiment with 100 Mbps modulation
  - >50 Mbps secret-key rate over 10-dB-loss channel
- Conclusions and plans for CONQUEST work

Essence of Floodlight QKD

- FL-QKD is two-way CVQKD with binary modulation
  - Alice sends unmodulated, continuous-wave (cw) light to Bob
  - Bob modulates and amplifies the light he receives from Alice
  - Alice homodyne detects her received light using a stored reference
- Low-brightness, broadband source used for key generation
  – transmit N_S<<1 photon/mode for immunity to passive eavesdropping
    cf. BB84, which transmits at most ~1 photon/bit to ensure security
  – use M >> 1 modes/bit so that MN_S >> 1 photons/bit are transmitted
    cf. classical communication, which transmits many photons/bit
- Photon-pair source used for security against collective attack
  - Alice and Bob's channel monitors determine Eve's intrusion parameter
  - knowing that f_E parameter they can bound her Holevo information

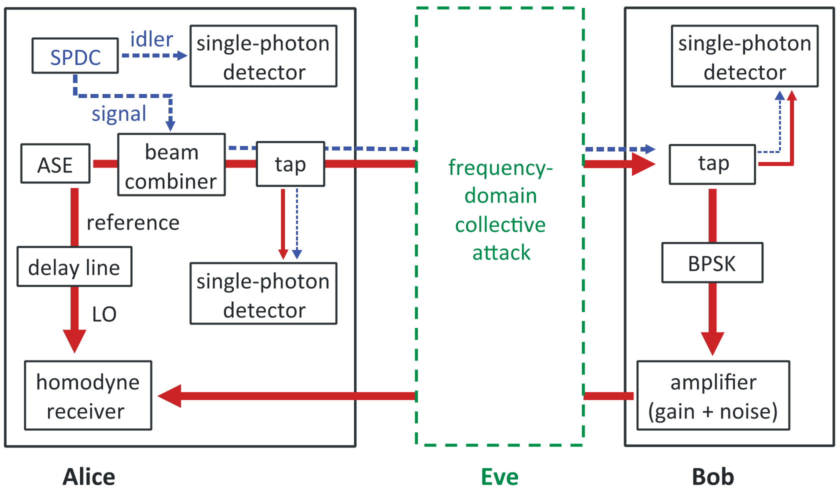
Floodlight QKD Protocol



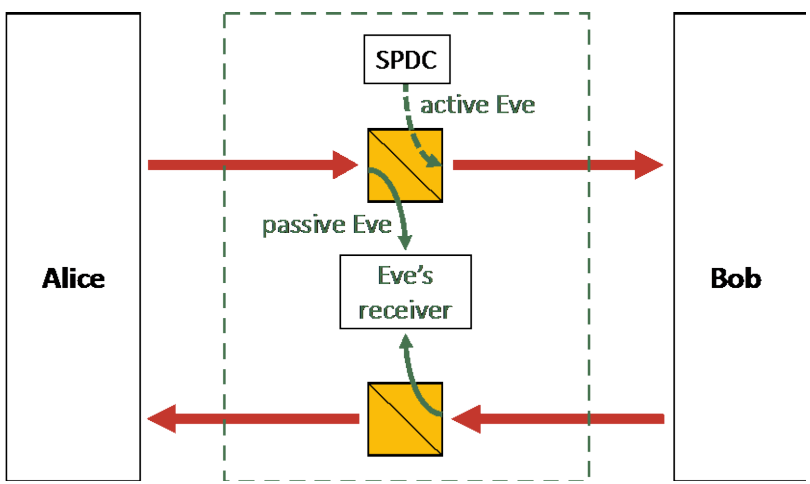
- Alice's SPDC and ASE brightnesses: $N_{SPDC} << N_S << 1$
- Alice's SPDC and ASE bandwidths: W
- Bob's bit rate: $R = 1/T << W$ implies $M = TW >> 1$ modes/bit

Security Analysis: Frequency-Domain Collective Attack

- Freq-Domain Collective Attack



- Realization of optimum version



- Freq-Domain Collective Attack
  - Eve replaces lossy fibers with lossless fibers and beam splitters
  - Eve does (K+1)-mode unitary transformation of light Alice sent
  - Eve transmits one output to Bob and retains the others
  - Eve taps light from Bob-to-Alice channel for joint measurement with light tapped from Alice-to-Bob fiber and retained K ancillas
- Realization of optimum version
  - Eve replaces lossy fibers with lossless fibers and beam splitters
  - Eve uses cw SPDC source of bandwidth W
  - Eve injects signal light into Bob
  - Eve retains idler light for joint measurement with light tapped from Alice-to-Bob and Bob-to-Alice fibers
  - f_E = Eve's light injection fraction

Security Analysis: Channel Monitors

- Singles and coincidence rates

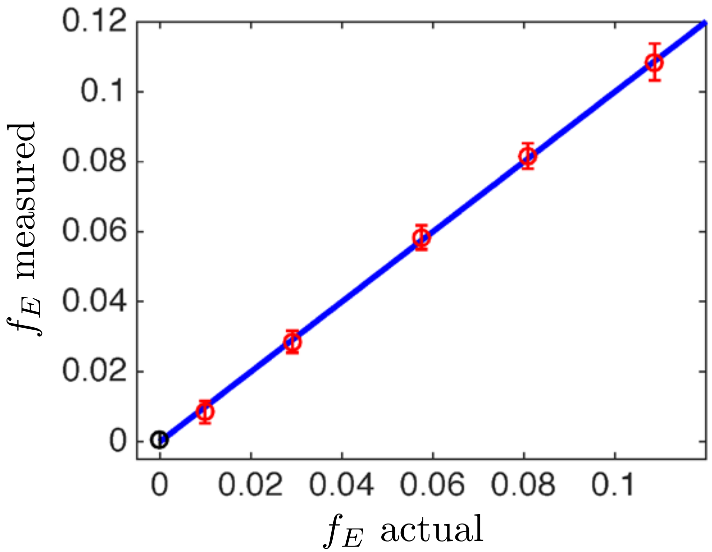
$$S_A = \text{Alice's signal-tap singles rate}$$
$$S_B = \text{Bob's signal-tap singles rate}$$
$$C_{IA} = \text{Alice's idler}\times\text{signal-tap time-aligned coincidence rate}$$
$$\widetilde{C}_{IA} = \text{Alice's idler}\times\text{signal-tap time-shifted coincidence rate}$$
$$C_{IB} = \text{Alice's idler}\times\text{Bob's signal-tap time-aligned coincidence rate}$$
$$\widetilde{C}_{IB} = \text{Alice's idler}\times\text{Bob's signal-tap time-shifted coincidence rate}$$

- Estimating f_E from these rates

$$f_E = 1 - \frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A}$$

  - measurement is calibration free

- Preliminary experiment

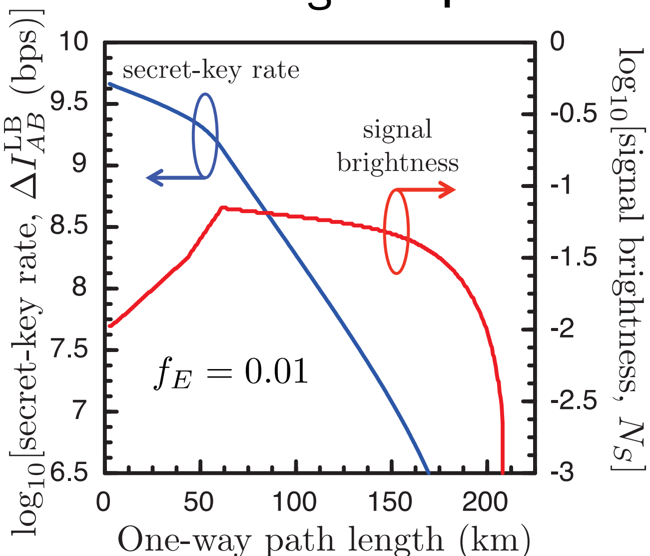


Theory: Zhuang *et al*., Phys. Rev. A **94,** 012322 (2016)

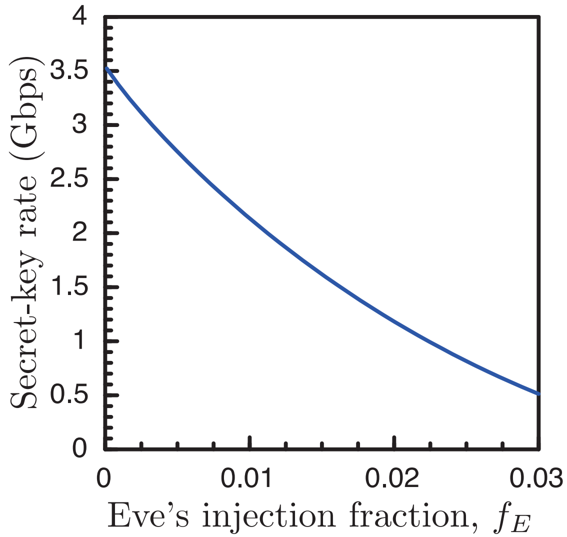
Experiment: Zhang *et al*., Phys. Rev. A **95,** 012332 (2017)

Secret-Key Rates (SKRs): Optimum Frequency-Domain Collective Attack

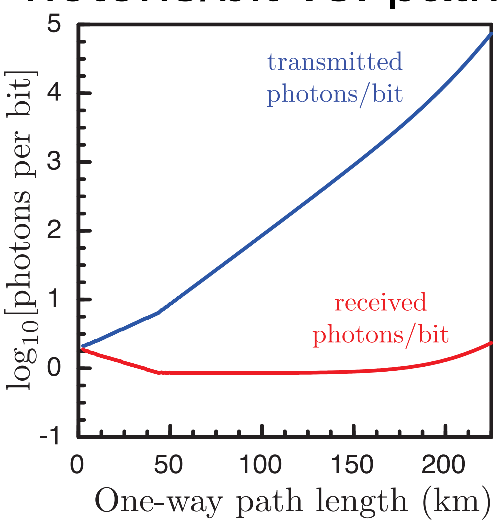
- SKR and N_S vs. path length



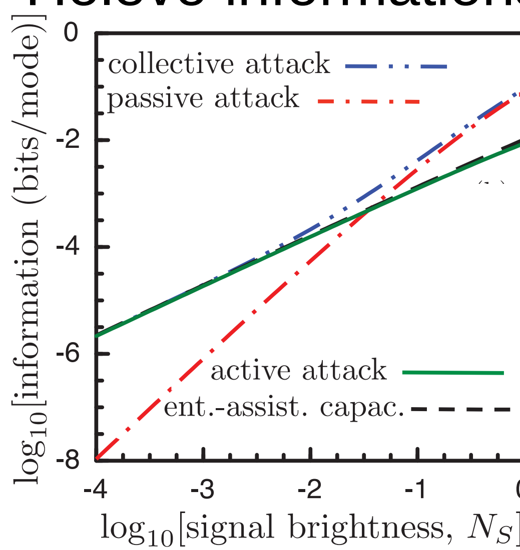
- SKR vs. f_E at 50 km



- Photons/bit vs. path length



- Holevo informations at 50 km

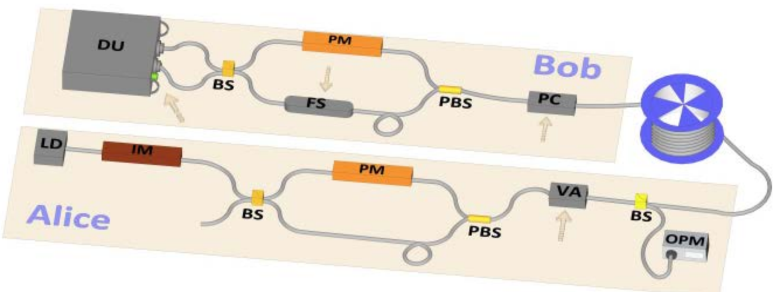


Zhuang *et al.*, Phys. Rev. A **94,** 012322 (2016)

Secret-Key Efficiency (SKE): State-of-the-Art Long-Distance, High-Rate Systems

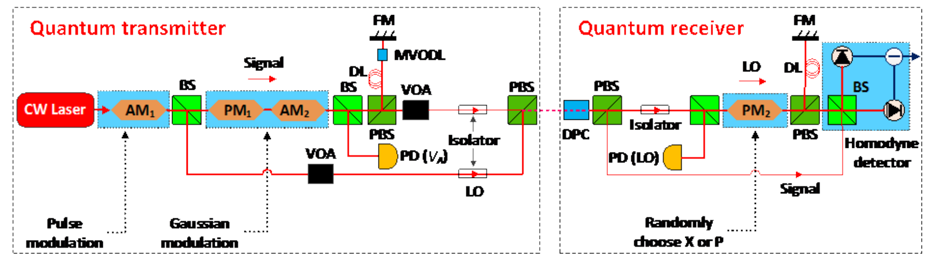
- SKE = secret-key rate in bits/channel-use
- State-of-the-art for long-distance, high-rate QKD
- discrete-variable QKD (DVQKD)
- continuous-variable QKD (CVQKD)

Lucamarini *et al*., Opt. Express 2013



decoy-state BB84 with 1 Gbps modulation
1 Mbps secret-key rate on 50-km fiber link

Huang *et al*., Opt. Express 2015



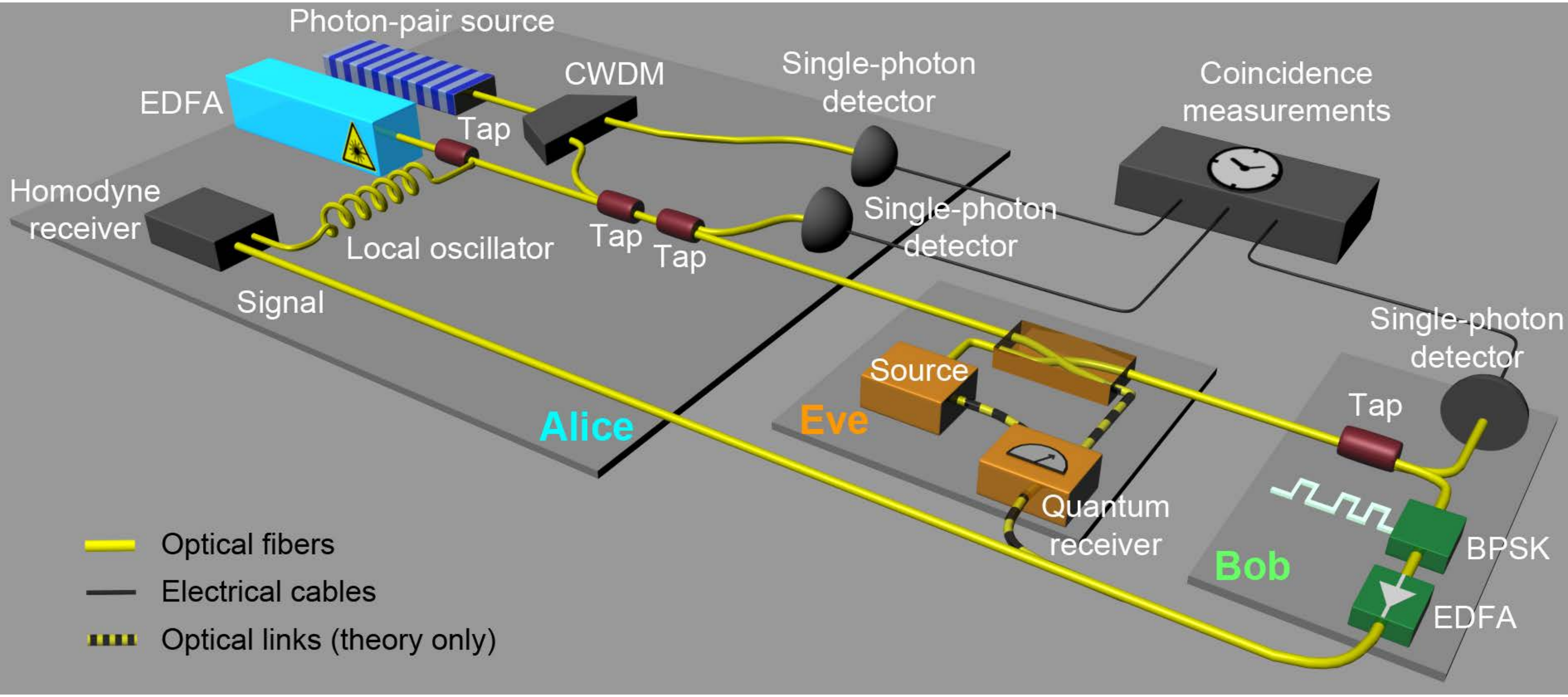
CVQKD with 50 Mbaud modulation
1 Mbps secret-key rate on 25-km fiber link

- Lucamarini *et al*.: SKE = 10^{-3} bits/channel-use
- Huang *et al*.: SKE = 1.8×10^{-3} bits/channel-use
- Ultimate limit for 10 dB channel loss*: SKE = 0.15 bits/*mode*

*Pirandola *et al*., arXiv:1510.08863 [quant-ph]

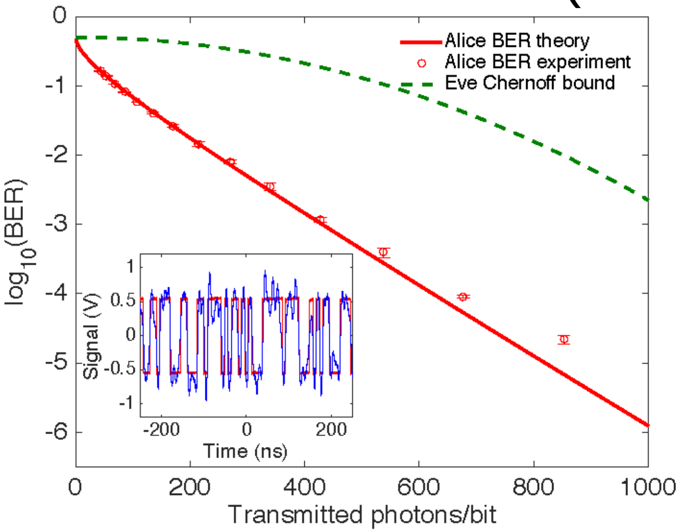
Proof-of-Principle Experiment: Setup

- 100 Mbps modulation, 10 dB propagation-loss channel

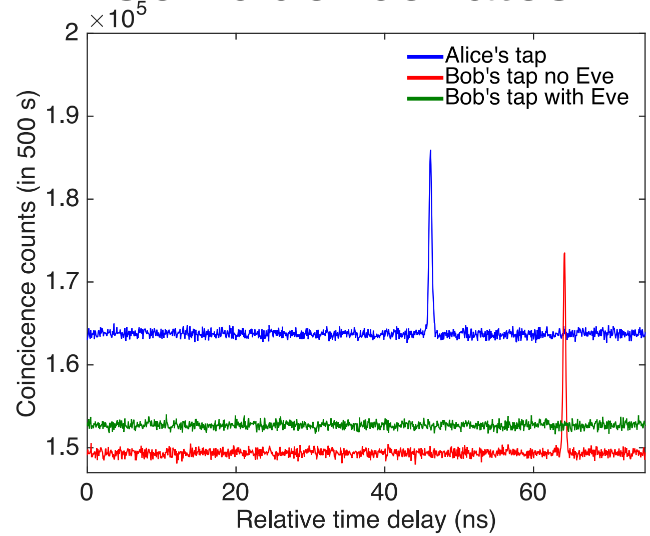


Proof-of-Principle Experiment: Results

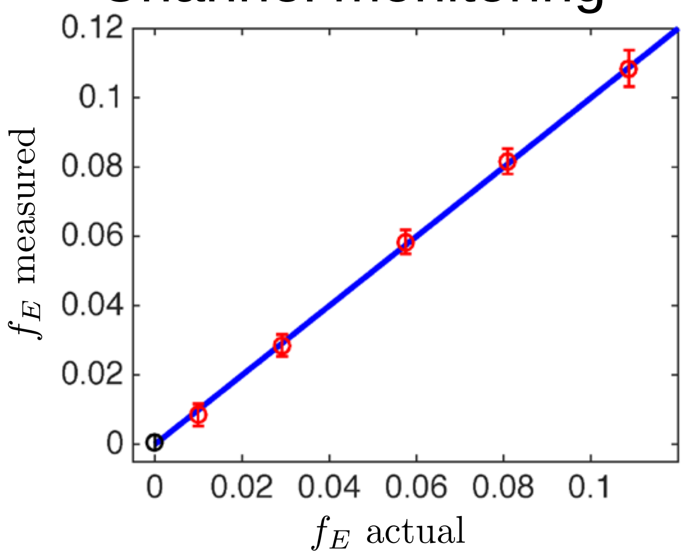
- Alice's bit-error rate (BER)



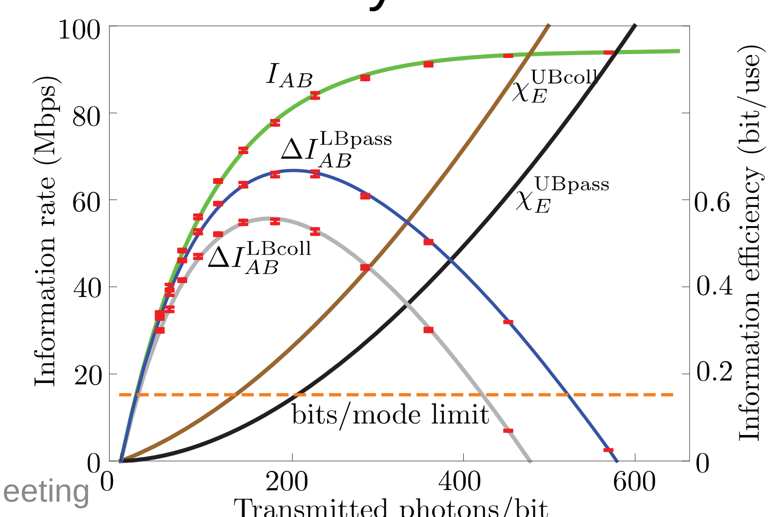
- Coincidence rates



- Channel monitoring



- Secret-key rates



Zhang *et al.*, Phys Rev A **95,** 012332 (2017)

FL-QKD: A Practical Route to Gbps Secret-Key Rates

- FL-QKD is two-way CVQKD with binary modulation
  - but its characteristics are very different from current CVQKD systems
- FL-QKD attractive option for metropolitan-area QKD
  - Gbps secret-key rates at 50 km possible *with*out new technology
  - existing systems would require extensive WDM to do so
- FL-QKD floods Alice-to-Bob fiber with many photons per bit
  - low brightness (photons/mode << 1) gives immunity to passive attack
  - broadband (modes/bit >> 1) yields many photons/bit for high rate
  - channel monitoring bounds Eve's collective-attack information
- Future work — AFOSR MURI and ONR CONQUEST sponsorship
  - higher-bandwidth homodyne receiver for Gbps demonstration
  - security analysis for coherent attacks including finite-key effects
  - protocol modification for higher secret-key efficiency

FL-QKD CONQUEST WORK

- Line-of-sight atmospheric path
  - absorption, scattering, and turbulence effects
  - near-field versus far-field power transfer
- Quantum communication protocol
  - QKD versus active + passive attack
  - Direct communication versus passive attack
- Energy-collection models for Eve
  - All energy lost in the quantum channels
  - Energy collected from a realistic field of view
- Attack models
  - active + passive coherent, collective, or individual attack
  - passive collective or individual attack

Preliminary Results: FL-QKD Secret-Key Rates

- Lower bounds on ergodic secret-key rates (SKRs)

FL-QKD SKRs				
height	decile	780 nm wavelength	1550 nm wavelength	4000 nm wavelength
19 m	10%	0.809 Gbps	0.907 Gbps	0.447 Gbps
19 m	50%	66.75 Mbps	97.33 Mbps	72.71 Mbps
19 m	90%	0.721 Mbps	1.50 Mbps	2.33 Mbps
30 m	10%	2.94 Gbps	2.66 Gbps	0.723 Gbps
30 m	50%	0.450 Gbps	0.585 Gbps	0.319 Gbps
30 m	90%	9.76 Mbps	19.66 Mbps	27.60 Mbps
50 m	10%	4.97 Gbps	4.04 Gbps	0.827 Gbps
50 m	50%	1.26 Gbps	1.43 Gbps	0.528 Gbps
50 m	90%	30.19 Mbps	58.83 Mbps	73.42 Mbps

  – average transmissivities: McBryde & Hammel extinction + turbulence profiles and a constant-intensity focused beam
  – FL-QKD SKR lower bound: 10 Gbps modulation, individual passive attack with Eve using an optimum quantum receiver on all the light that doesn't reach its intended destination

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

A non-Gaussian CVQKD protocol for three signal states

Kamil Brádler, Christian Weedbrook

CipherQ

Continuous-variable QKD

- Continuous equivalent of DVQKD
- Secret key encoded in the complementary observables X and P
- Advantages: high bit rates, experimental realization
- Disadvantages: Security analysis not as mature as for DVQKD, classical postprocessing slow
- Main focus so far: Gaussian CVQKD – Gaussian states chosen with a Gaussian prior in phase space
- Only in that case the adversary's (Eve) most general attack is known – a Gaussian operation
- How about Gaussian states chosen discretely?
- Advantages: HW and random number generation simpler
- A few discrete states suspected to quickly approach Gaussian modulation

Binary modulated CVQKD

- The signal states are Gaussian (coherent states $|\alpha_0\rangle, |\alpha_1\rangle$) with $p_0 = p_1 = 1/2$
- The signals are sent down a quantum channel in order to establish private classical correlations (secret key)
- Eve's best strategy is unknown
- Nothing is assumed about the adversary except that the attack is *collective* and the protocol *asymptotic*
- A formula for a lower bound on the secret key provided
- It only depends on easily measurable quantities
- Calculated for a lossy bosonic channel (rate a fcn of a channel transmissivity)

Zhao et. al. PRA 79, 012307 (2009)

Ternary modulated CVQKD

- Main object of study is the following density matrix

$$A = p_0|\alpha_0\rangle\langle\alpha_0| + p_1|\alpha_1\rangle\langle\alpha_1| + p_2|\alpha_2\rangle\langle\alpha_2|$$

- $p_0 = p_1 = p_2 = 1/3$ and α_i are coherent signal states
- Three and more signals are qualitatively different from the two-signal case
- Even if we choose symmetric $|\alpha_i\rangle$, Eve's states ψ_i^y conditioned on Bob's announcement Y (public) are not guaranteed to satisfy the imposed symmetries
- In addition, a major technical roadblock ahead

Entropy calculations

- Let's follow the binary proof strategy as much as we can
- The key rate is obtained by maximizing

$$H(E|X)_\varrho + H(X:E)_\varrho - H(E|Y)_\varrho$$

$H(E|Y) = \sum_y p_y H(\varrho_E^y)$

✓ $H(E|X), H(X:E)$

- For $H(X:E)$ one diagonalizes

$$\varrho_E = \frac{1}{3}(|\alpha_0\rangle\langle\alpha_0| + |\alpha_1\rangle\langle\alpha_1| + |\alpha_2\rangle\langle\alpha_2|)$$

- For $H(E|Y)$ it is

$$\varrho_E^y = p(0|y)|\psi_0^y\rangle\langle\psi_0^y| + p(1|y)|\psi_1^y\rangle\langle\psi_1^y| + p(2|y)|\psi_2^y\rangle\langle\psi_2^y|$$

Entropy calculations

- No brute-force diagonalization but instead the Cayley-Hamilton theorem was used
- The coeffs in $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ are given by $\sum_n \mathrm{Tr}[\varrho_E^n]$
- The eigenvalues depend on Eve's states

$$\langle \psi_i^y | \psi_j^y \rangle = z_{ij} \in \mathbb{C}$$

- In order to see whether the calculation is manageable we set $z_{ij} = z \in (0,1)$ (ignoring the phase)
- To restore full generality, the phase will be added or argued to be irrelevant
- For now ϱ_E^y is a function of z and $p(k|y), y = \{0,1,2\}$

Monotonicity and concavity of h_3

- The second major step was to show that $H(\varrho_E^y)$ is monotone-decreasing and concave in z for all $p(k|y)$
- The main ingredients to lower bound the secret key rates
- The original paper analyzed the binary Shannon entropy for $0 \leq u \leq 1/2$

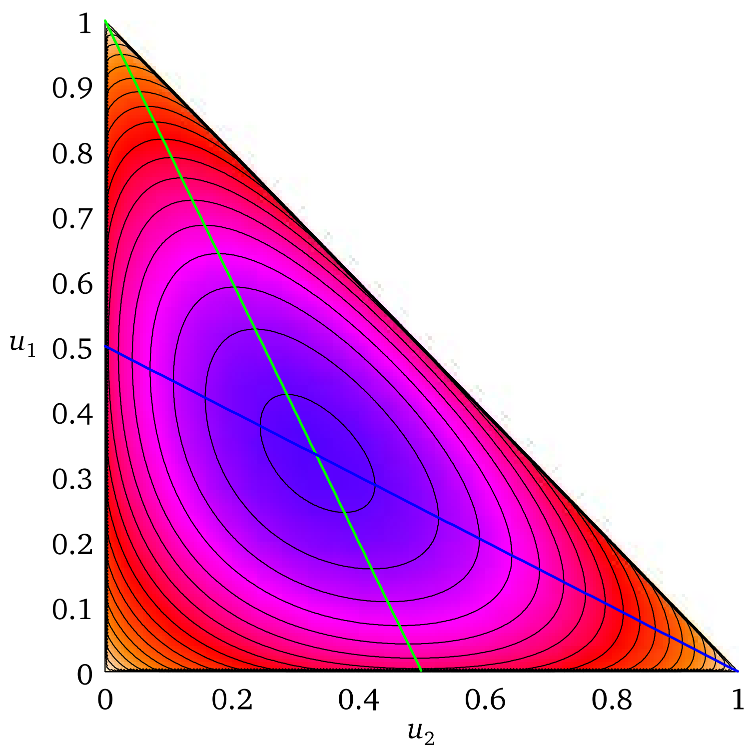
$$H(\varrho_E^y) = h_2(u(z;p)) = -u \log u - (1-u) \log [1-u]$$

- We study the ternary Shannon entropy

$$h_3(\vec{u}(z;\vec{p})) = -u_1 \log u_1 - u_2 \log u_2 - (1-u_1-u_2) \log [1-u_1-u_2]$$

- There is a HUGE difference between h_2 and h_3

Monotonicity and concavity of h_3



- We showed that h_3 is monotone-decreasing and concave in z for all $p(k|y)$

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Distribution Statement A. Approved for Public Release

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Efficient post-processing for CV QKD

Saikat Guha
BBN

Review Meeting
Feb 17, 2017

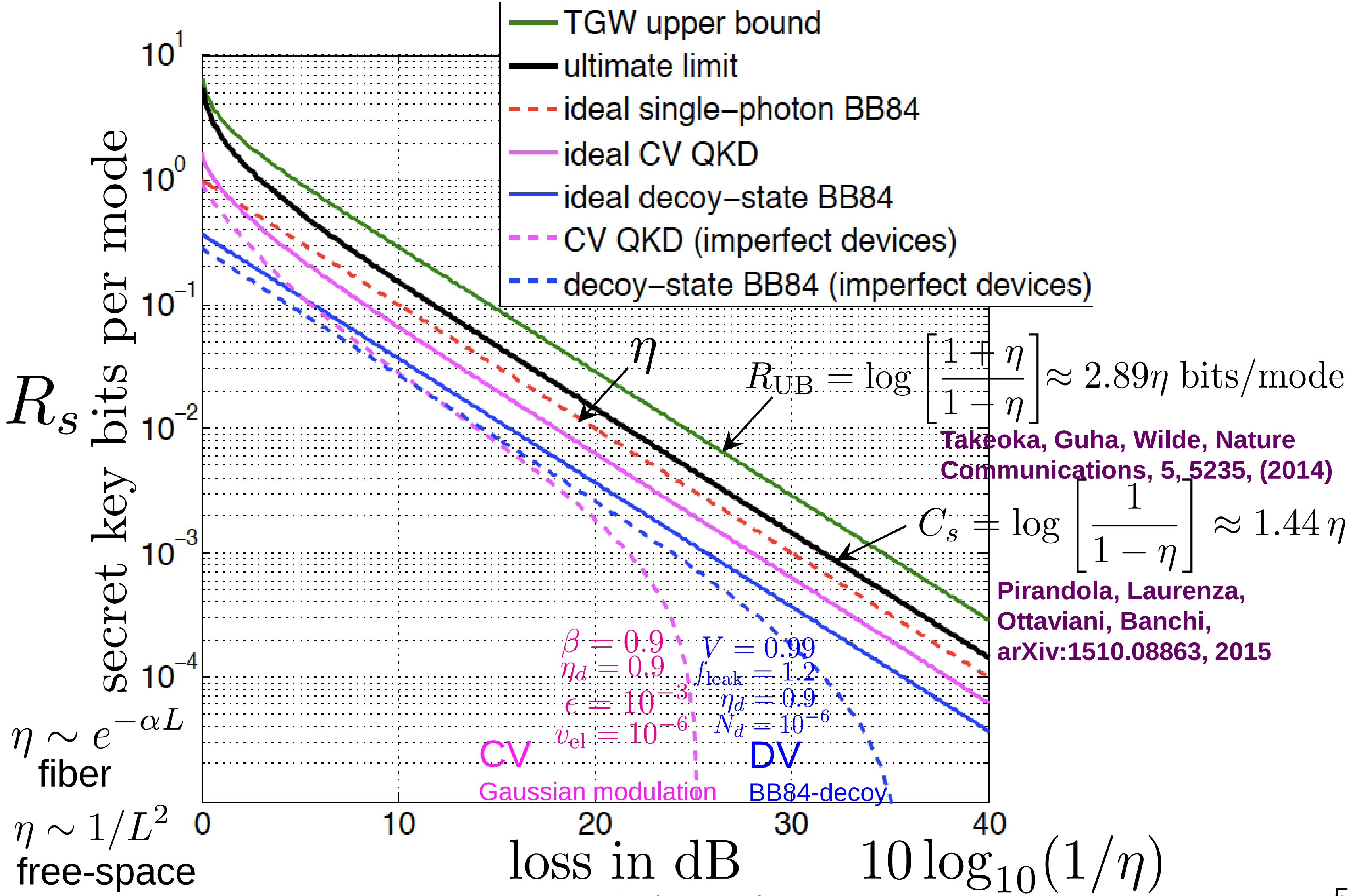
Outline

- **Free-space QKD: near-to-far field transition**
  - Rate-vs.-loss of direct transmission QKD protocols
  - Multiple spatial modes to maximize rate for short-range deployment
- **Continuous variable QKD**
  - Efficient post-processing methods for CV QKD
    - Discrete modulation with guard band post processing
    - Floodlight QKD and block post processing for CV QKD

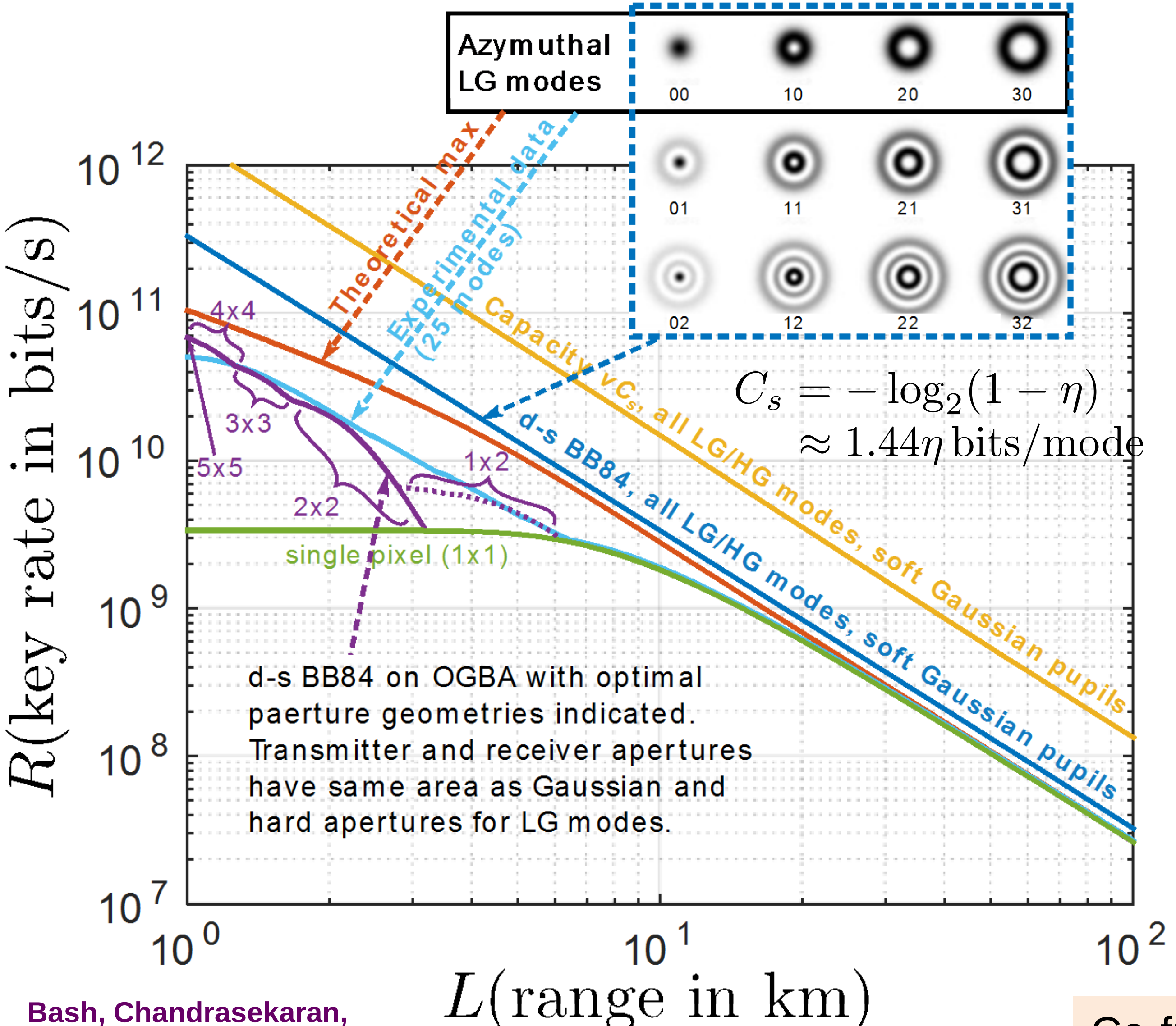
Outline

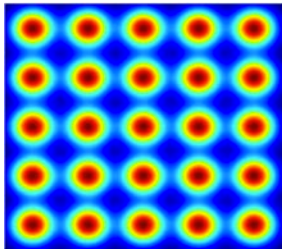
- **Free-space QKD: near-to-far field transition**
  - Rate-vs.-loss of direct transmission QKD protocols
  - Multiple spatial modes to maximize rate for short-range deployment
- **Continuous variable QKD**
  - Efficient post-processing methods for CV QKD
    - Discrete modulation with guard band post processing
    - Floodlight QKD and block post processing for CV QKD

Rate-vs.-loss for direct-transmission QKD



Multiple spatial modes: near-to-far field





Focused beams

- Multiple spatial modes can help at short ranges: higher rate improvement at shorter wavelengths (more modes)

- Don't quite need orthogonal (e.g., OAM) modes; overlapping focused beams work pretty well

$$r_t = r_r = 7\,\mathrm{cm}$$
$$\lambda = 1.55\mu\mathrm{m}$$
$$P_d = 10^{-6}$$
$$\nu = 10\mathrm{GHz}$$
$$V = 0.99$$

Bash, Chandrasekaran, Shapiro, Guha, arxiv:1604.08582

Co-funded by Sandia National Laboratory

Outline

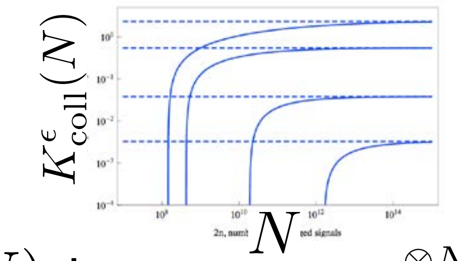
- **Free-space QKD: near-to-far field transition**
  - Rate-vs.-loss of direct transmission QKD protocols
  - Multiple spatial modes to maximize rate for short-range deployment
- **Continuous variable QKD**
  - Efficient post-processing methods for CV QKD
    - Discrete modulation with guard band post processing
    - Floodlight QKD and block post processing for CV QKD

CV QKD: status of security proofs

- What do we mean by a “QKD protocol is secure”?
  - Work in the equivalent “entanglement based” picture (vs. P&M)

$$\rho_{A^N B^N} \rightarrow \frac{1}{2}\left\| \rho_{K_A K_B E} - \frac{1}{2^l}\sum_{s\in\{0,1\}^l} |s,s\rangle\langle s,s| \otimes \rho_E \right\|_1 \leq \epsilon$$

Key rate: $$K^\epsilon(N) = \max_{\{\text{postprocessing}\}} \frac{l}{N}$$



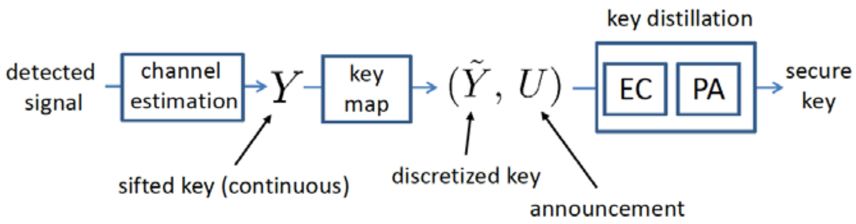
  - Key rate with “collective attack” assumption $K^\epsilon_{\text{coll}}(N)$, i.e. $\rho_{A^N B^N} = \rho_{AB}^{\otimes N}$
  - Everyone calculates this: $K^{\text{asymp}}_{\text{coll}} = \max_{N_S} [\beta I(A;B) - \chi(B,E)] \times W$
  - Gaussian modulation: security against collective attacks proven [Leverrier, 2015], and $K^\epsilon_{\text{coll}}(N) \approx K^{\text{asymp}}_{\text{coll}}$ for N ~ 10^{10} – 10^{14}
  - Only two parameters (loss and noise) need to be estimated
  - But no useful finite-length key-rate LB, i.e., $K^\epsilon(N) \geq 0$
- Discrete-modulation (2-state and 4-state): $K^{\text{asymp}}_{\text{coll}}$ known, but is not proven to be achievable: optimal “attack” not known

CV QKD: status of security proofs (contd.)

- Input power, reconciliation efficiency, constellation cardinality

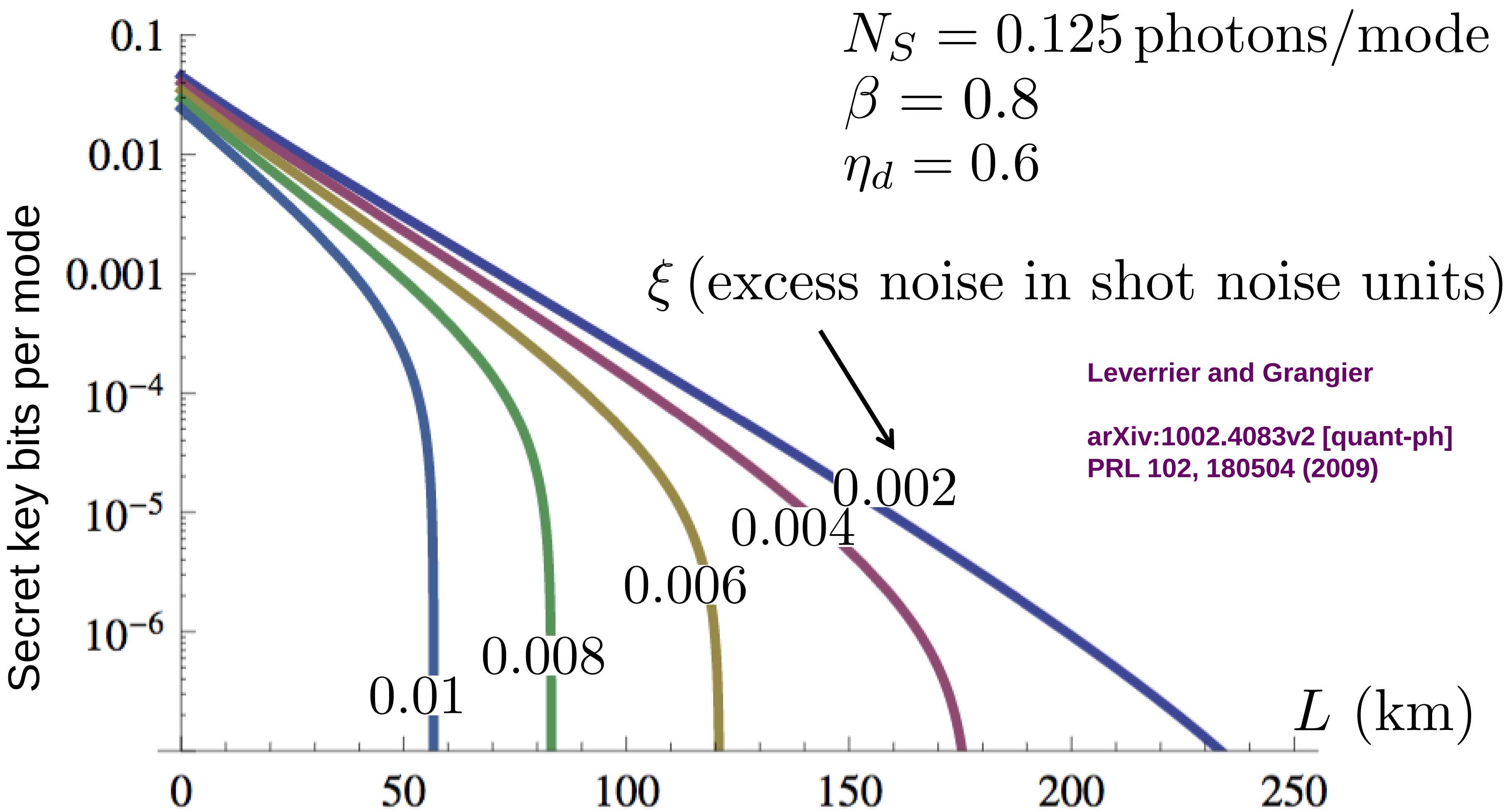
$$K_{\text{coll}}^{\text{asymp}} = \max_{N_S} \left[\beta I(A;B) - \chi(B,E)\right] \times W$$

  - I(A;B) – χ(B;E) → (optimal) const. N_S → ∞; β<1, optimal N_S goes down
  - Good ECC (high β) at low N_S hard to achieve:
    - (1) recent progress (β ~ 0.96: multi-edge LDPC codes, Gaussian mod.)
    - (2) discrete constellation: high β easier; simpler transmitter (no need for Gaussian when N_S small), PP overhead, may get better range, “0” hitting
  - Short distances (low loss): High N_S better – multi-state constellation
- Post-processing overhead vs. key rate



  - Every single mode generates “data” that gets fed into post-processing: unlike in DV QKD, only η fraction of modes generates clicks
  - When the channel is lossy, do we really need to feed data from each detected mode into post-processing (key map)?

Discrete 4-state modulation ($K_{\text{coll}}^{\text{asymp}}$)



Leverrier and Grangier

arXiv:1002.4083v2 [quant-ph]
PRL 102, 180504 (2009)

If we assume "linear" channel, collective-attack security known

QKD with binary phase modulation

- BPSK coherent state modulation + heterodyne
  - Rate lower bound known with general collective attack

$X \quad |\pm\alpha\rangle \quad \boxed{\eta} \quad |\pm\sqrt{\eta}\alpha\rangle \quad$ Heterodyne $\quad \boldsymbol{y} = (y_1, y_2)$

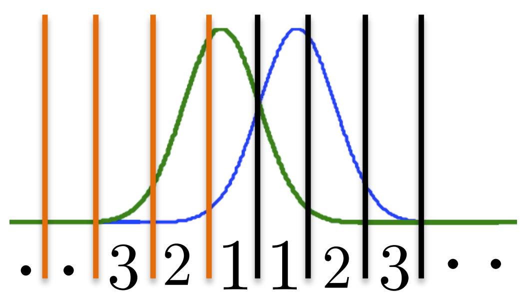
Alice — Eve — Bob

$$|\pm\sqrt{1-\eta}\alpha\rangle$$

Zhao, Heid, Rigas, Lutkenhaus, PRA 79, 012307 (2009)

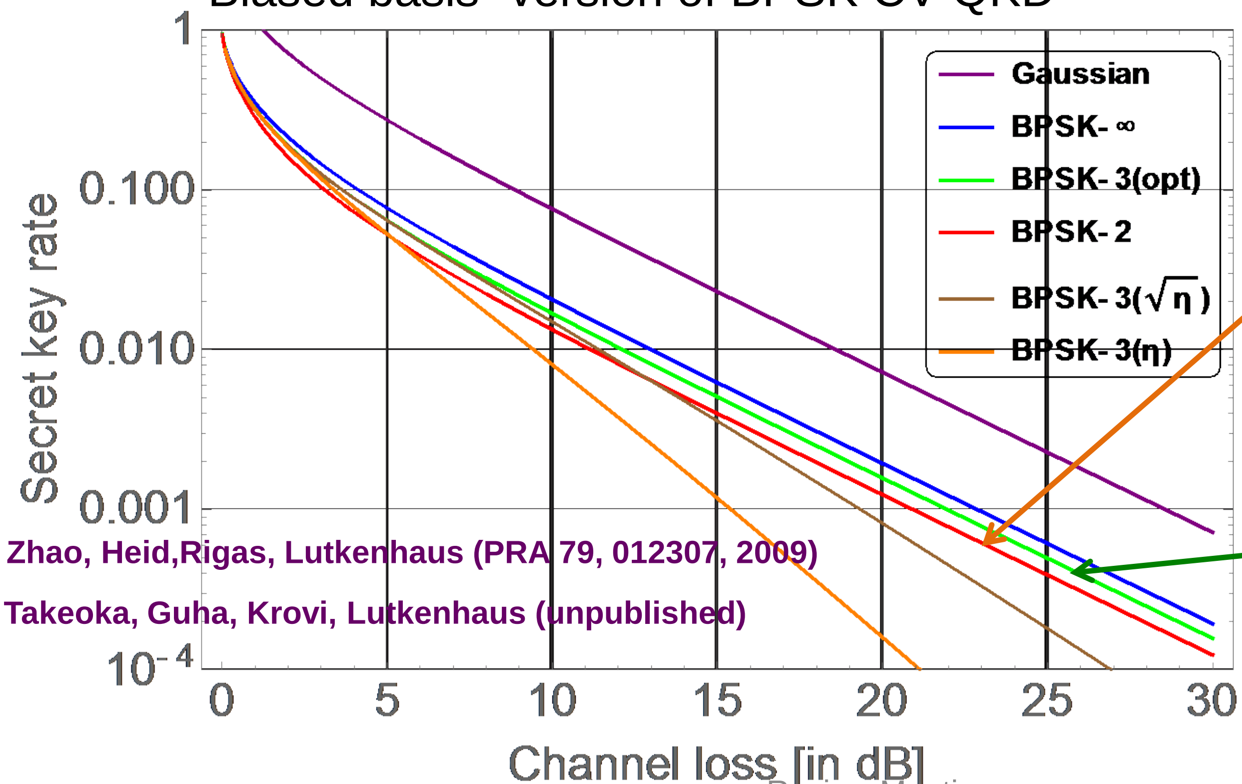
$$P[\mathcal{E}=1] = \epsilon = \frac{1}{2}\mathrm{erfc}(\sqrt{2\eta|\alpha|^2})$$

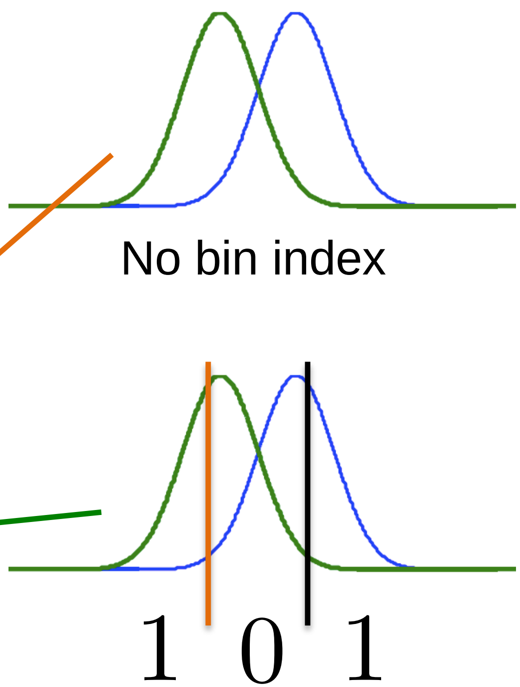
  - Key map: (Announcement, Discretization)
    - Discretization = $\mathrm{sign}(y_1)$ → gets fed into post-processing
    - Announcement = $(|y_1|, y_2)$
      - The noise "bin index" $u = |y_1|$ requires infinite precision



Trade rate with post-processing overhead

- Key results so far:
  - Optimal key map for BPSK + Heterodyne for noiseless lossy channel
  - 2-bin PP (get rid of the infinite-res bin index entirely)
  - 3-bin PP (1 bit bin-index): nothing to announce on a large fraction of modes
  - "Biased basis" version of BPSK CV QKD





Discrete modulation: ongoing work

- Table-top FSO experiment for BPSK CV QKD
- Potential paths to rate LB with finite constellations
  - Extending Zhao et. al.'s technique (Kamil Bradler, Christian Weedbrook)
  - Extending Fabian Furrer's Entropic Uncertainly techniques
  - Extending IQC numerical technique (Patrick Coles, Norbert Lutkenhaus)
  - Anthony Leverrier's CV-decoy ideas (don't work in current form)
- Constellation cardinality that achieves "pretty much" the performance of Gaussian modulation at a given channel loss
- Key rate LB with finite key length (Mark Wilde, Saikat Guha)

Note: No modulation is "Gaussian" due to finite extinction ratio of EOMs and finite RNG (it is always a discrete modulation)

Block post-processing

- If Bob employs a M-length block of raw data in a repetition code, SNR roughly becomes M fold higher
- (Bits per M-length-symbol) / M = bits/mode not much worse than M = 1 bits/mode, but could save PP overhead, achieve better β
- This idea of an inner repetition code (or block post-processing) was first proposed by Leverrier and Grangier in (PRL 102, 180504, 2009) for CV QKD with 2-PSK and 4-PSK

0.99 0.82 -0.04 1.53 **-0.91** -0.94 0.41 0.97 **-0.29** -1.49 0.37 -0.02 **-1.02** -1.06 -0.26 0.69 **-0.81** 0.77 -2.65 -0.65 **-1.02** 1.06 -0.26 0.69 …

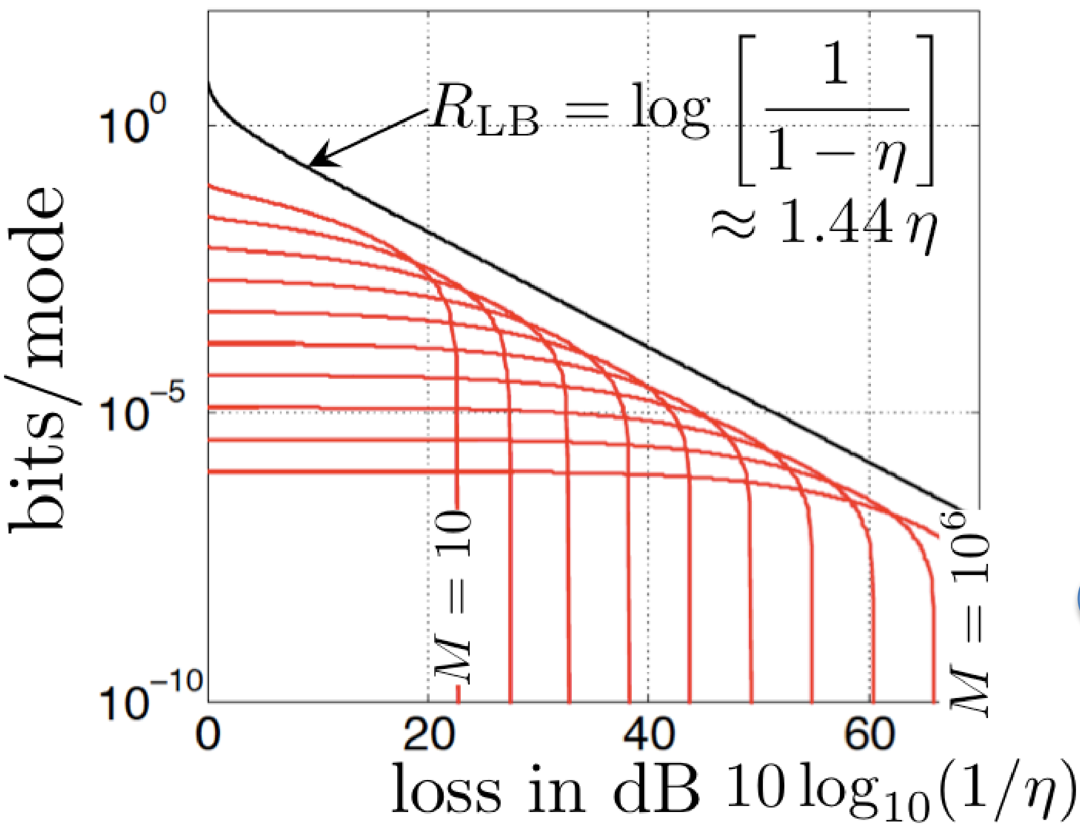
- Instead of Bob announcing the sign of each, he announces the sign of the first measurement in a (k=4) block relative to the others in the block

1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, …

- Reverse reconciliation version of M=4 repetition code (1,1,1,1 vs. -1,-1,-1,-1)

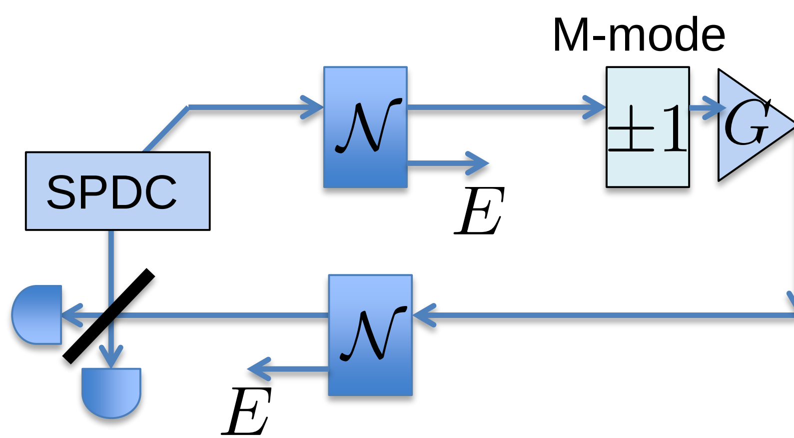
Block post-processing vis-à-vis FL-QKD

- Alice uses a THz optical BW source, Bob uses a GHz BW binary phase modulator (block length M ~ 1000), THz modes/sec



Proposed by Jeff Shapiro et al. arXiv:1607.00457

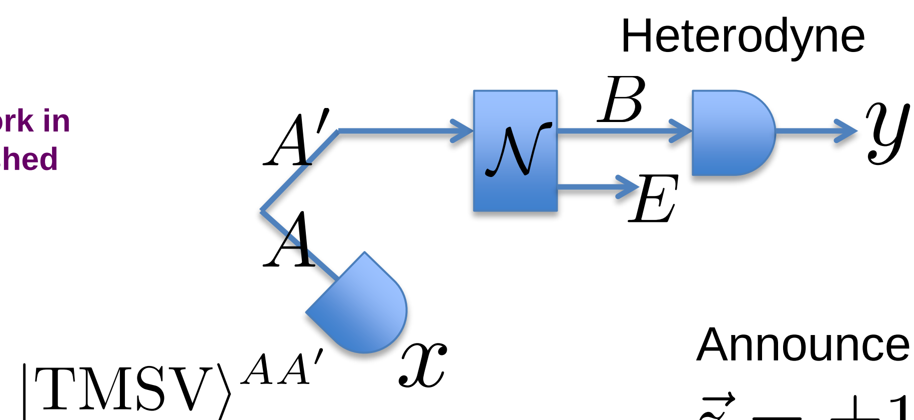
- Leverages block post-processing
- Two-way channel (reverse optical channel only for a practical purpose)
- $K_{\mathrm{coll}}^{\mathrm{asymp}}$ known, $K^{\epsilon}(N) = ?$



CV QKD with block post-processing

- FL-QKD (almost) mathematically equivalent to standard Gaussian modulated CV QKD with a block post-processing, but with a HUGE modes/s advantage
- Proving security ($K^{\epsilon}(N) = ?$) of CV QKD with this new key map may prove security for FL-QKD and vice versa

Guha, Takeoka; work in progress, unpublished (2017)



Announcement

$$\vec{z} = \pm 1(\vec{y}) + \vec{n}$$

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Converse bounds for private communication over quantum channels

Mark M. Wilde (LSU)

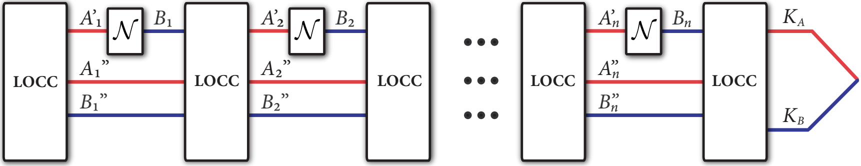
joint work with Mario Berta (Caltech) and
Marco Tomamichel ($|$Univ. Sydney$\rangle$ + $|$Univ. of Technology, Sydney$\rangle$)

arXiv:1602.08898
accepted for publication in IEEE Trans. Inf. Theory
DOI: 10.1109/TIT.2017.2648825

February 17, 2017

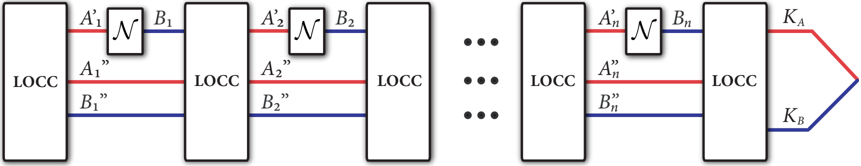
Setup I

- Given a quantum channel $\mathcal{N}$ and a quantum key distribution (**QKD**) protocol that uses it n times, how much **key** can be generated?



Setup I

- Given a quantum channel $\mathcal{N}$ and a quantum key distribution (**QKD**) protocol that uses it n times, how much **key** can be generated?



- **Ideal secret key**:

$$\overline{\Phi}_{AB} \otimes \sigma_E \equiv \frac{1}{K} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E. \quad (1)$$

Approximate secret key: A state ρ_{ABE} is an ε-close secret key if $F(\rho_{ABE}, \overline{\Phi}_{AB} \otimes \sigma_E) \geq 1 - \varepsilon$, where F denotes quantum fidelity.

Setup II

- **Non-asymptotic private capacity**: maximum rate of ε-close secret key achievable using the channel n times with two-way classical communication (LOCC) assistance

$$\boxed{\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon) := \sup\left\{P : (n,P,\varepsilon) \text{ is achievable for } \mathcal{N} \text{ using LOCC}\right\}. \qquad (2)}$$

Setup II

- **Non-asymptotic private capacity**: maximum rate of ε-close secret key achievable using the channel n times with two-way classical communication (LOCC) assistance

$$\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon) := \sup\left\{P : (n, P, \varepsilon) \text{ is achievable for } \mathcal{N} \text{ using LOCC}\right\}. \quad (2)$$

- The idea is to fix $n \geq 1$ and $\varepsilon \in (0,1)$ and then determine how large the secret key rate can be.

Setup III

- Practical question: how to characterize $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n,\varepsilon)$ for all $n \geq 1$ and $\varepsilon \in (0,1)$? The answers give the **fundamental limitations of QKD**.

Setup III

- Practical question: how to characterize $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n, \varepsilon)$ for all $n \geq 1$ and $\varepsilon \in (0, 1)$? The answers give the **fundamental limitations of QKD**.

- Upper bounds on $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n, \varepsilon)$ can be used as **benchmarks for quantum repeaters** [Lütkenhaus].

Setup III

- Practical question: how to characterize $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n, \varepsilon)$ for all $n \geq 1$ and $\varepsilon \in (0, 1)$? The answers give the **fundamental limitations of QKD**.

- Upper bounds on $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n, \varepsilon)$ can be used as **benchmarks for quantum repeaters** [Lütkenhaus].

- Today, I will present

  the tightest known upper bound on $\hat{P}^{\leftrightarrow}_{\mathcal{N}}(n, \varepsilon)$

  for several channels of practical interest. Interesting special case: single-mode phase-insensitive bosonic Gaussian channels.

Overview

1. Main Results (Examples)

2. Proof Idea: Meta Converse

Main Result: Gaussian Channels I

- Converse bounds for single-mode phase-insensitive bosonic Gaussian channels, most importantly the **photon loss channel**

$$\mathcal{L}_\eta : \ \hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e} \tag{3}$$

where transmissivity $\eta \in [0,1]$ and environment in vacuum state.

Main Result: Gaussian Channels I

- Converse bounds for single-mode phase-insensitive bosonic Gaussian channels, most importantly the **photon loss channel**

$$\mathcal{L}_\eta : \ \hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e} \tag{3}$$

where transmissivity $\eta \in [0,1]$ and environment in vacuum state.

- Our approach gives a complete proof for the following weak converse bound, stated in [Pirandola *et al.* 2016]:

$$P^{\leftrightarrow}(\mathcal{L}_\eta) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) , \tag{4}$$

which is actually tight in the asymptotic limit, i.e., $P^{\leftrightarrow}(\mathcal{L}_\eta) = \log\left(\frac{1}{1-\eta}\right)$.

- Converse bounds for single-mode phase-insensitive bosonic Gaussian channels, most importantly the **photon loss channel**

$$\mathcal{L}_\eta : \; \hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e} \tag{3}$$

  where transmissivity $\eta \in [0,1]$ and environment in vacuum state.

- Our approach gives a complete proof for the following weak converse bound, stated in [Pirandola *et al.* 2016]:

$$P^{\leftrightarrow}(\mathcal{L}_\eta) := \lim_{\varepsilon\to 0} \lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) , \tag{4}$$

  which is actually tight in the asymptotic limit, i.e., $P^{\leftrightarrow}(\mathcal{L}_\eta) = \log\left(\frac{1}{1-\eta}\right)$. The weak-converse bound follows from a finite-length bound:

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \frac{\log\left(\frac{1}{1-\eta}\right) + 2h_2(\varepsilon)/n}{(1-8\varepsilon)} \tag{5}$$

- Converse bounds for single-mode phase-insensitive bosonic Gaussian channels, most importantly the **photon loss channel**

$$\mathcal{L}_\eta : \ \hat{b} = \sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{e} \tag{3}$$

where transmissivity $\eta \in [0,1]$ and environment in vacuum state.

- Our approach gives a complete proof for the following weak converse bound, stated in [Pirandola *et al.* 2016]:

$$P^{\leftrightarrow}(\mathcal{L}_\eta) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right), \tag{4}$$

which is actually tight in the asymptotic limit, i.e., $P^{\leftrightarrow}(\mathcal{L}_\eta) = \log\left(\frac{1}{1-\eta}\right)$. The weak-converse bound follows from a finite-length bound:

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \frac{\log\left(\frac{1}{1-\eta}\right) + 2h_2(\varepsilon)/n}{(1-8\varepsilon)} \tag{5}$$

- Drawback: an asymptotic statement, and thus says **little for practical protocols** (called a weak converse bound).

- We show the **non-asymptotic converse bound**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n}, \tag{6}$$

where $C(\varepsilon) := \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$ (other choices possible).

Main Result: Gaussian Channels II

- We show the **non-asymptotic converse bound**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n}, \qquad (6)$$

where $C(\varepsilon) := \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$ (other choices possible).

- This bound implies the strong converse: $\lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right)$.

Main Result: Gaussian Channels II

- We show the **non-asymptotic converse bound**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n}, \tag{6}$$

where $C(\varepsilon) := \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$ (other choices possible).

- This bound implies the strong converse: $\lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right)$.
- Can be used to **assess the performance of any practical quantum repeater** which uses a loss channel n times for desired security ε.

Main Result: Gaussian Channels II

- We show the **non-asymptotic converse bound**

$$\boxed{\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n}, \qquad (6)}$$

where $C(\varepsilon) := \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$ (other choices possible).

- This bound implies the strong converse: $\lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right)$.
- Can be used to **assess the performance of any practical quantum repeater** which uses a loss channel n times for desired security ε.
- Other variations of this bound are possible if η is not the same for each channel use, if η is chosen adversarially, etc.

Main Result: Gaussian Channels II

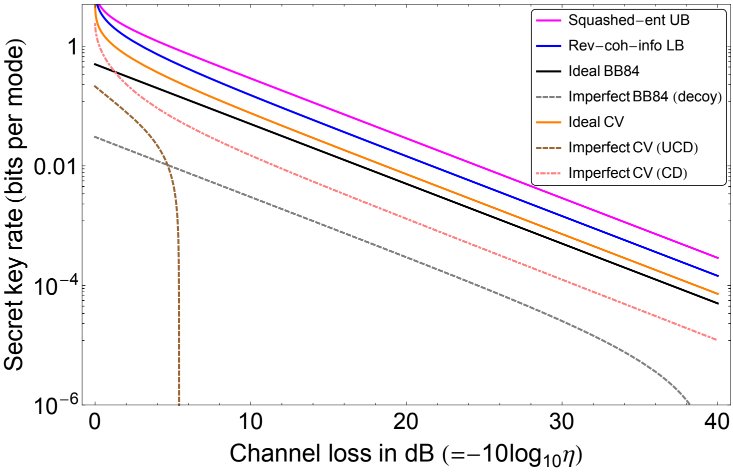
- We show the **non-asymptotic converse bound**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n}, \tag{6}$$

where $C(\varepsilon) := \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$ (other choices possible).

- This bound implies the strong converse: $\lim_{n\to\infty} \hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right)$.
- Can be used to **assess the performance of any practical quantum repeater** which uses a loss channel n times for desired security ε.
- Other variations of this bound are possible if η is not the same for each channel use, if η is chosen adversarially, etc.
- We give similar bounds for the quantum-limited amplifier channel (tight), thermalizing channels, amplifier channels, and additive noise channels.

Fundamental rate-loss trade-off from [TGW14]



Can translate x-axis to km by assuming fiber has 0.2 dB loss / km

Main Result: Dephasing Channels I

- Asymptotic result [Pirandola *et al.* 2016] for the **qubit dephasing channel**

$$\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\,\rho + \gamma Z \rho Z$$

with $\gamma \in (0,1)$ is

$$P^{\leftrightarrow}(\mathcal{Z}_\gamma) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{Z}_\gamma}(n, \varepsilon) = 1 - h(\gamma)\,, \tag{7}$$

with the binary entropy $h(\gamma) := -\gamma \log \gamma - (1-\gamma)\log(1-\gamma)$.

- Asymptotic result [Pirandola *et al.* 2016] for the **qubit dephasing channel**

$$\mathcal{Z}_\gamma : \rho \mapsto (1-\gamma)\,\rho + \gamma Z \rho Z$$

with $\gamma \in (0,1)$ is

$$P^{\leftrightarrow}(\mathcal{Z}_\gamma) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \hat{P}^{\leftrightarrow}_{\mathcal{Z}_\gamma}(n,\varepsilon) = 1 - h(\gamma)\,, \tag{7}$$

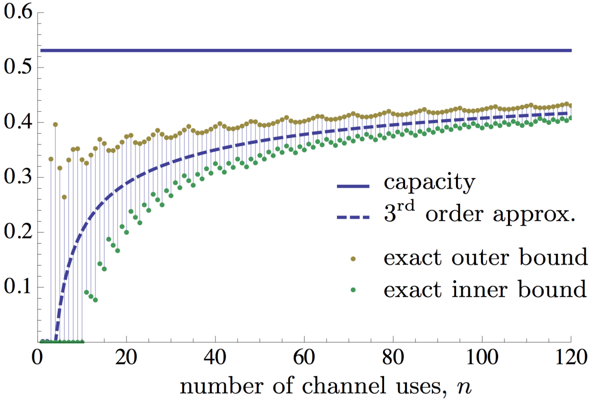
with the binary entropy $h(\gamma) := -\gamma \log \gamma - (1-\gamma)\log(1-\gamma)$.

- By combining with [Tomamichel *et al.* 2016] we show the expansion

$$\boxed{\hat{P}^{\leftrightarrow}_{\mathcal{Z}_\gamma}(n,\varepsilon) = 1 - h(\gamma) + \sqrt{\frac{v(\gamma)}{n}}\,\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\left(\frac{1}{n}\right)\,, \qquad (8)}$$

with Φ the cumulative standard Gaussian distribution and the binary entropy variance $v(\gamma) := \gamma(\log \gamma + h(\gamma))^2 + (1-\gamma)(\log(1-\gamma) + h(\gamma))^2$.

- For the dephasing parameter $\gamma = 0.1$ we get (figure from [Tomamichel *et al.* 2016]):



(c) Comparison of strict bounds with third order approximation for $\varepsilon = 5\%$.

Proof Idea: Meta Converse I

- **Meta converse approach** from classical channel coding [Polyanskiy *et al.* 2010], uses connection to **hypothesis testing**. In the quantum regime, e.g., for classical communication [Tomamichel & Tan 2015] or quantum communication [Tomamichel *et al.* 2014 & 2016]. We extend this approach to **private communication**.

Proof Idea: Meta Converse I

- **Meta converse approach** from classical channel coding [Polyanskiy *et al.* 2010], uses connection to **hypothesis testing**. In the quantum regime, e.g., for classical communication [Tomamichel & Tan 2015] or quantum communication [Tomamichel *et al.* 2014 & 2016]. We extend this approach to **private communication**.
- Hypothesis testing relative entropy defined for a state ρ, positive semi-definite operator σ, and $\varepsilon \in [0,1]$ as

$$D_H^{\varepsilon}(\rho\|\sigma) := -\log \inf \left\{ \operatorname{Tr}[\Lambda\sigma] : 0 \leq \Lambda \leq I \wedge \operatorname{Tr}[\Lambda\rho] \geq 1-\varepsilon \right\}. \tag{9}$$

- **Meta converse approach** from classical channel coding [Polyanskiy *et al.* 2010], uses connection to **hypothesis testing**. In the quantum regime, e.g., for classical communication [Tomamichel & Tan 2015] or quantum communication [Tomamichel *et al.* 2014 & 2016]. We extend this approach to **private communication**.
- Hypothesis testing relative entropy defined for a state ρ, positive semi-definite operator σ, and $\varepsilon \in [0,1]$ as

$$D_H^{\varepsilon}(\rho\|\sigma) := -\log\inf\left\{\operatorname{Tr}[\Lambda\sigma] : 0 \leq \Lambda \leq I \wedge \operatorname{Tr}[\Lambda\rho] \geq 1-\varepsilon\right\}. \tag{9}$$

- The ε-relative entropy of entanglement is defined as

$$E_R^{\varepsilon}(A;B)_\rho := \inf_{\sigma_{AB}\in\mathcal{S}(A:B)} D_H^{\varepsilon}(\rho_{AB}\|\sigma_{AB}), \tag{10}$$

  where $\mathcal{S}(A:B)$ is the set of separable states (cf. relative entropy of entanglement). **Channel's ε-relative entropy of entanglement** is then given as

$$\boxed{E_R^{\varepsilon}(\mathcal{N}) := \sup_{|\psi\rangle_{AA'}\in\mathcal{H}_{AA'}} E_R^{\varepsilon}(A;B)_\rho,} \tag{11}$$

  where $\rho_{AB} := \mathcal{N}_{A'\to B}(\psi_{AA'})$.

Proof Idea: Meta Converse II

- Goal is the creation of $\log K$ **bits of key**, i.e., states γ_{ABE} with

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E \qquad (12)$$

for some state σ_E and measurement channels $\mathcal{M}_A, \mathcal{M}_B$.

Proof Idea: Meta Converse II

- Goal is the creation of $\log K$ **bits of key**, i.e., states γ_{ABE} with

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K} \sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E \qquad (12)$$

  for some state σ_E and measurement channels $\mathcal{M}_A, \mathcal{M}_B$.

- In **one-to-one correspondence** with pure states $\gamma_{AA'BB'E}$ such that [Horodecki *et al.* 2005 & 2009]

$$\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U^\dagger_{ABA'B'}\,, \qquad (13)$$

  where Φ_{AB} maximally entangled, $U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'}$ with each $U^{ij}_{A'B'}$ a unitary, and $\theta_{A'B'}$ a state.

Proof Idea: Meta Converse II

- Goal is the creation of $\log K$ **bits of key**, i.e., states γ_{ABE} with

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K}\sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E \qquad (12)$$

for some state σ_E and measurement channels $\mathcal{M}_A, \mathcal{M}_B$.

- In **one-to-one correspondence** with pure states $\gamma_{AA'BB'E}$ such that [Horodecki *et al.* 2005 & 2009]

$$\gamma_{ABA'B'} = U_{ABA'B'}(\Phi_{AB} \otimes \theta_{A'B'})U^{\dagger}_{ABA'B'}, \qquad (13)$$

where Φ_{AB} maximally entangled, $U_{ABA'B'} = \sum_{i,j} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{ij}_{A'B'}$ with each $U^{ij}_{A'B'}$ a unitary, and $\theta_{A'B'}$ a state.

- Work in the latter, bipartite picture.

- Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the "γ-privacy test" satisfies

$$\operatorname{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1-\varepsilon, \tag{14}$$

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB} \otimes I_{A'B'})U^{\dagger}_{ABA'B'}$ is a projective "γ-privacy test."

Proof Idea: Meta Converse III

- Let $\varepsilon \in [0, 1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the "γ-privacy test" satisfies

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1 - \varepsilon, \tag{14}$$

  where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB} \otimes I_{A'B'})U^{\dagger}_{ABA'B'}$ is a projective "γ-privacy test."
- For **separable states** $\sigma_{AA'BB'}$ (useless for private communication) and a state $\gamma_{AA'BB'}$ with $\log K$ bits of key we have [Horodecki *et al.* 2009]

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{AA'BB'}\} \leq \frac{1}{K}, \tag{15}$$

Proof Idea: Meta Converse III

- Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the "γ-privacy test" satisfies

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1-\varepsilon, \tag{14}$$

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB} \otimes I_{A'B'})U^{\dagger}_{ABA'B'}$ is a projective "γ-privacy test."

- For **separable states** $\sigma_{AA'BB'}$ (useless for private communication) and a state $\gamma_{AA'BB'}$ with $\log K$ bits of key we have [Horodecki *et al.* 2009]

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{AA'BB'}\} \leq \frac{1}{K}, \tag{15}$$

- The monotonicity of the channel's ε-relative entropy of entanglement $E_R^{\varepsilon}(\mathcal{N})$ with respect to LOCC together with (15) implies the **meta converse**

$$\boxed{\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N}) \quad \text{(LOCC pre- and post-processing assistance).} \quad (16)}$$

For n channel uses this gives $\hat{P}_{\mathcal{N}}(n,\varepsilon) \leq \frac{1}{n}E_R^{\varepsilon}(\mathcal{N}^{\otimes n})$.

Proof Idea: Meta Converse III

- Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the "γ-privacy test" satisfies

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1-\varepsilon, \tag{14}$$

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB} \otimes I_{A'B'})U^{\dagger}_{ABA'B'}$ is a projective "γ-privacy test."

- For **separable states** $\sigma_{AA'BB'}$ (useless for private communication) and a state $\gamma_{AA'BB'}$ with $\log K$ bits of key we have [Horodecki *et al.* 2009]

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{AA'BB'}\} \leq \frac{1}{K}, \tag{15}$$

- The monotonicity of the channel's ε-relative entropy of entanglement $E_R^{\varepsilon}(\mathcal{N})$ with respect to LOCC together with (15) implies the **meta converse**

$$\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N}) \quad \text{(LOCC pre- and post-processing assistance).} \tag{16}$$

For n channel uses this gives $\hat{P}_{\mathcal{N}}(n,\varepsilon) \leq \frac{1}{n}E_R^{\varepsilon}(\mathcal{N}^{\otimes n})$.

- Finite block-length version of **relative entropy of entanglement** upper bound [Horodecki *et al.* 2005 & 2009].

- Let $\varepsilon \in [0,1]$ and let $\rho_{ABA'B'}$ be an ε-approximate γ-private state. The probability for $\rho_{ABA'B'}$ to pass the "γ-privacy test" satisfies

$$\mathrm{Tr}\{\Pi_{ABA'B'}\rho_{ABA'B'}\} \geq 1-\varepsilon, \tag{14}$$

where $\Pi_{ABA'B'} \equiv U_{ABA'B'}(\Phi_{AB}\otimes I_{A'B'})U^{\dagger}_{ABA'B'}$ is a projective "γ-privacy test."

- For **separable states** $\sigma_{AA'BB'}$ (useless for private communication) and a state $\gamma_{AA'BB'}$ with $\log K$ bits of key we have [Horodecki *et al.* 2009]

$$\mathrm{Tr}\{\Pi_{ABA'B'}\sigma_{AA'BB'}\} \leq \frac{1}{K}, \tag{15}$$

- The monotonicity of the channel's ε-relative entropy of entanglement $E_R^{\varepsilon}(\mathcal{N})$ with respect to LOCC together with (15) implies the **meta converse**

$$\boxed{\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N}) \quad \text{(LOCC pre- and post-processing assistance).} \quad (16)}$$

For n channel uses this gives $\hat{P}_{\mathcal{N}}(n,\varepsilon) \leq \frac{1}{n}E_R^{\varepsilon}(\mathcal{N}^{\otimes n})$.

- Finite block-length version of **relative entropy of entanglement** upper bound [Horodecki *et al.* 2005 & 2009].
- One can then **evaluate** the meta converse for specific channels of interest.

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1, \varepsilon) \leq E_R^{\varepsilon}(\mathcal{N})$ gives bounds for the private transmission capabilities of quantum channels. These give the **fundamental limitations of QKD** and thus can be used as **benchmarks for quantum repeaters**.

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1, \varepsilon) \leq E_R^{\varepsilon}(\mathcal{N})$ gives bounds for the private transmission capabilities of quantum channels. These give the **fundamental limitations of QKD** and thus can be used as **benchmarks for quantum repeaters**.
- Can our bound be improved for the **photon loss channel**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n, \varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right) \tag{17}$$

to $C'(\varepsilon) := \log\left(\frac{1}{1-\varepsilon}\right)$?

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N})$ gives bounds for the private transmission capabilities of quantum channels. These give the **fundamental limitations of QKD** and thus can be used as **benchmarks for quantum repeaters**.
- Can our bound be improved for the **photon loss channel**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right) \tag{17}$$

  to $C'(\varepsilon) := \log\left(\frac{1}{1-\varepsilon}\right)$?
- Corresponding matching **achievability**? (Tight analysis of random coding in infinite dimensions needed.)

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N})$ gives bounds for the private transmission capabilities of quantum channels. These give the **fundamental limitations of QKD** and thus can be used as **benchmarks for quantum repeaters**.
- Can our bound be improved for the **photon loss channel**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right) \tag{17}$$

to $C'(\varepsilon) := \log\left(\frac{1}{1-\varepsilon}\right)$?

- Corresponding matching **achievability**? (Tight analysis of random coding in infinite dimensions needed.)
- Tight **finite-energy** bounds for single-mode phase-insensitive bosonic Gaussian channels?

Conclusion

- Our meta converse $\hat{P}_{\mathcal{N}}(1,\varepsilon) \leq E_R^{\varepsilon}(\mathcal{N})$ gives bounds for the private transmission capabilities of quantum channels. These give the **fundamental limitations of QKD** and thus can be used as **benchmarks for quantum repeaters**.
- Can our bound be improved for the **photon loss channel**

$$\hat{P}^{\leftrightarrow}_{\mathcal{L}_\eta}(n,\varepsilon) \leq \log\left(\frac{1}{1-\eta}\right) + \frac{C(\varepsilon)}{n} \quad \text{with} \quad C(\varepsilon) = \log 6 + 2\log\left(\frac{1+\varepsilon}{1-\varepsilon}\right) \tag{17}$$

  to $C'(\varepsilon) := \log\left(\frac{1}{1-\varepsilon}\right)$?
- Corresponding matching **achievability**? (Tight analysis of random coding in infinite dimensions needed.)
- Tight **finite-energy** bounds for single-mode phase-insensitive bosonic Gaussian channels?
- Understand more channels, for example such with $P^{\leftrightarrow} > 0$ but zero quantum capacity [Horodecki *et al.* 2008]?

Plan forward

- We suspect it should be possible to use the technique of Muller-Hermes *et al.* in arXiv:1604.03448 to derive bounds for protocols using finite energy. This would give tighter bounds.
- We are generalizing these upper bound methods such that they could apply more specifically to floodlight quantum key distribution (work in progress)
- We are working on applying these bounds to particular protocols commonly used in quantum key distribution

- For **Gaussian channels** we need formulas for the relative entropy $D(\rho\|\sigma)$ and the relative entropy variance $V(\rho\|\sigma)$.
- From [Chen 2005, Pirandola *et al.* 2015] and [Wilde *et al.* 2016], respectively: writing zero-mean Gaussian states in exponential form as

$$\rho = Z_\rho^{-1/2} \exp\left\{-\frac{1}{2}\hat{x}^T G_\rho \hat{x}\right\} \quad \text{with} \tag{18}$$

$$Z_\rho := \det(V^\rho + i\Omega/2), \quad G_\rho := 2i\Omega \operatorname{arcoth}(2V^\rho i\Omega)\,, \tag{19}$$

and V^ρ the Wigner function covariance matrix for ρ, we have

$$D(\rho\|\sigma) = \frac{1}{2}\left(\log\left(\frac{Z_\sigma}{Z_\rho}\right) - \operatorname{Tr}\left[\Delta V^\rho\right]\right) \tag{20}$$

$$V(\rho\|\sigma) = \frac{1}{2}\operatorname{Tr}\{\Delta V^\rho \Delta V^\rho\} + \frac{1}{8}\operatorname{Tr}\{\Delta\Omega\Delta\Omega\}\,, \tag{21}$$

where $\Delta := G_\rho - G_\sigma$.

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Chip-based quantum key distribution for maritime applications

Darius Bunandar, Dirk Englund
MIT

ONR CONQUEST Review
February 17, 2017

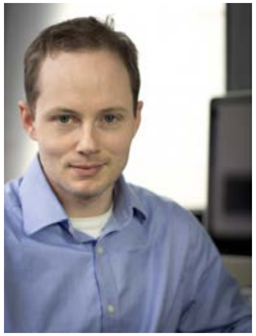
Outline

- **High-dimensional temporal QKD**: optimization of secret key capacity
- **Chip-based Tx/Rx for maritime QKD**:
  - Programmable dispersion for HD-QKD and dynamic dispersion control
  - Chip design for adaptive transmitters and receivers
  - Polarization-based QKD
- **Summary**

Acknowledgments

- **Quantum Photonics Group:**
- **Professor Dirk Englund**
- Catherine Lee, Mihika Prabhu, Nick Harris, Greg Steinbrecher, Darius Bunandar

- **Collaborators:**
- **MIT**: Prof. Jeffrey Shapiro, Dr. Franco Wong, Dr. Z. Zhang
- **Sandia National Laboratories**: Junji Urayama, Nicholas Boynton, Nicholas Martinez, Christopher DeRose, Anthony Lentine, Paul Davids, Ryan Camacho
- **MIT Lincoln Laboratory**: P. Ben Dixon, Scott A. Hamilton


Dirk Englund


Catherine Lee

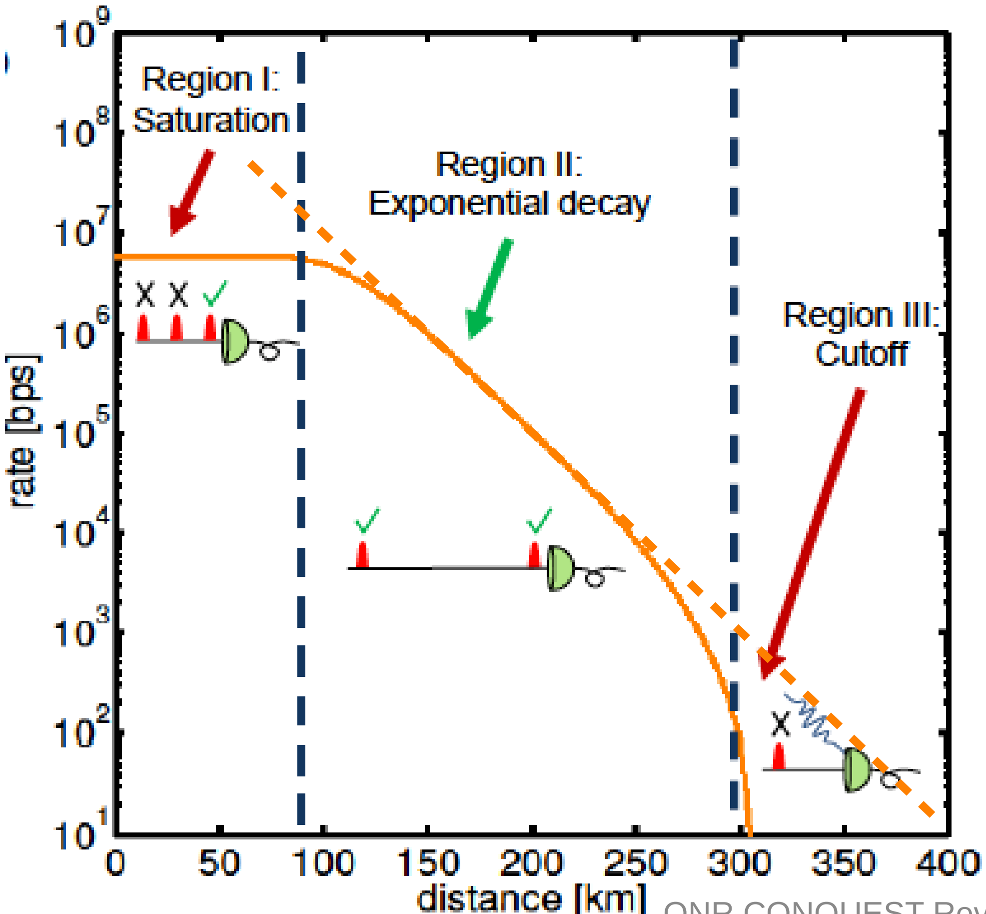

Mihika Prabhu


Nick Harris


Greg Steinbrecher

Detector limitations

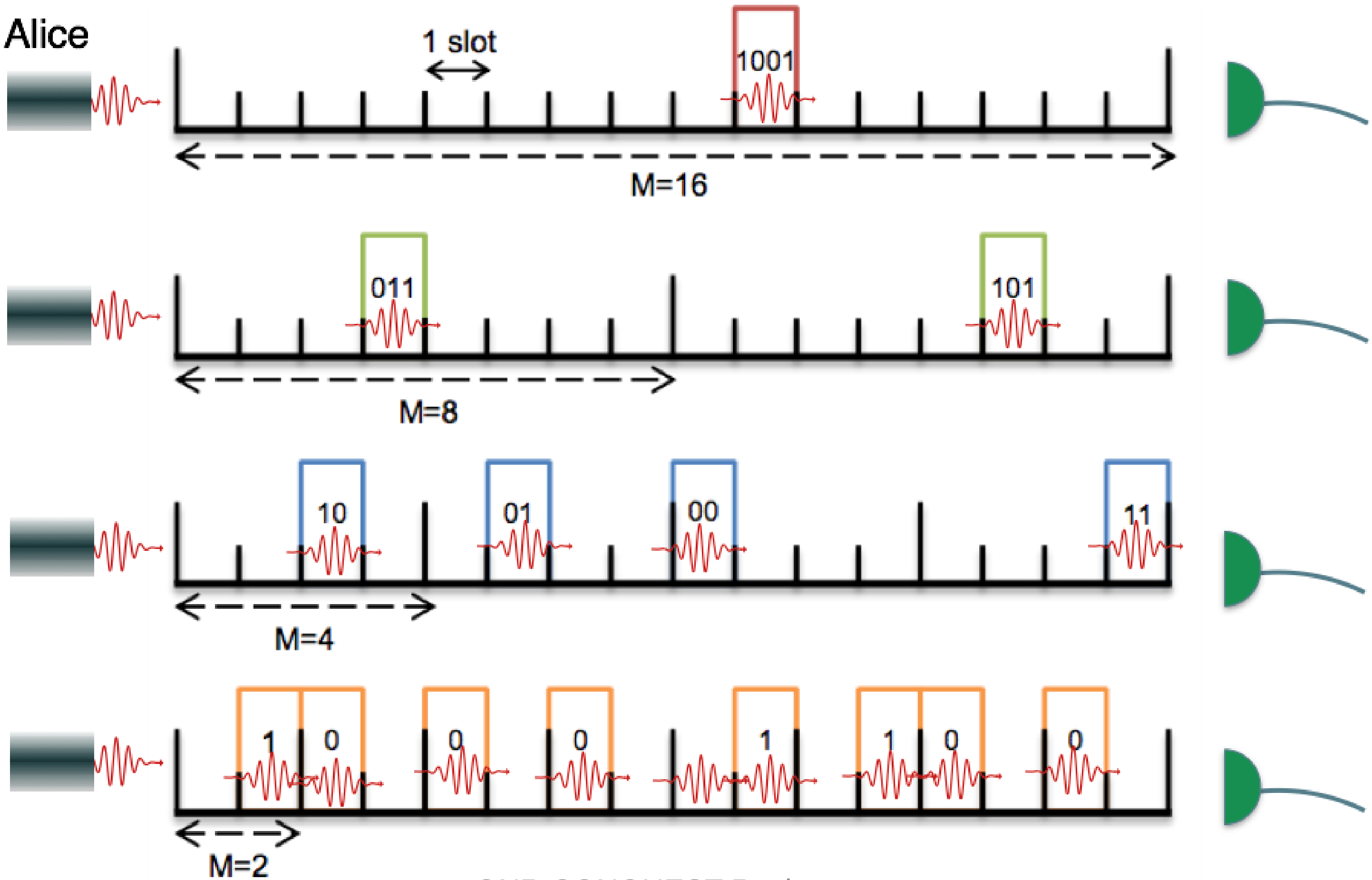
- QKD, at short distances, is limited by detector saturation (and/or source brightness)



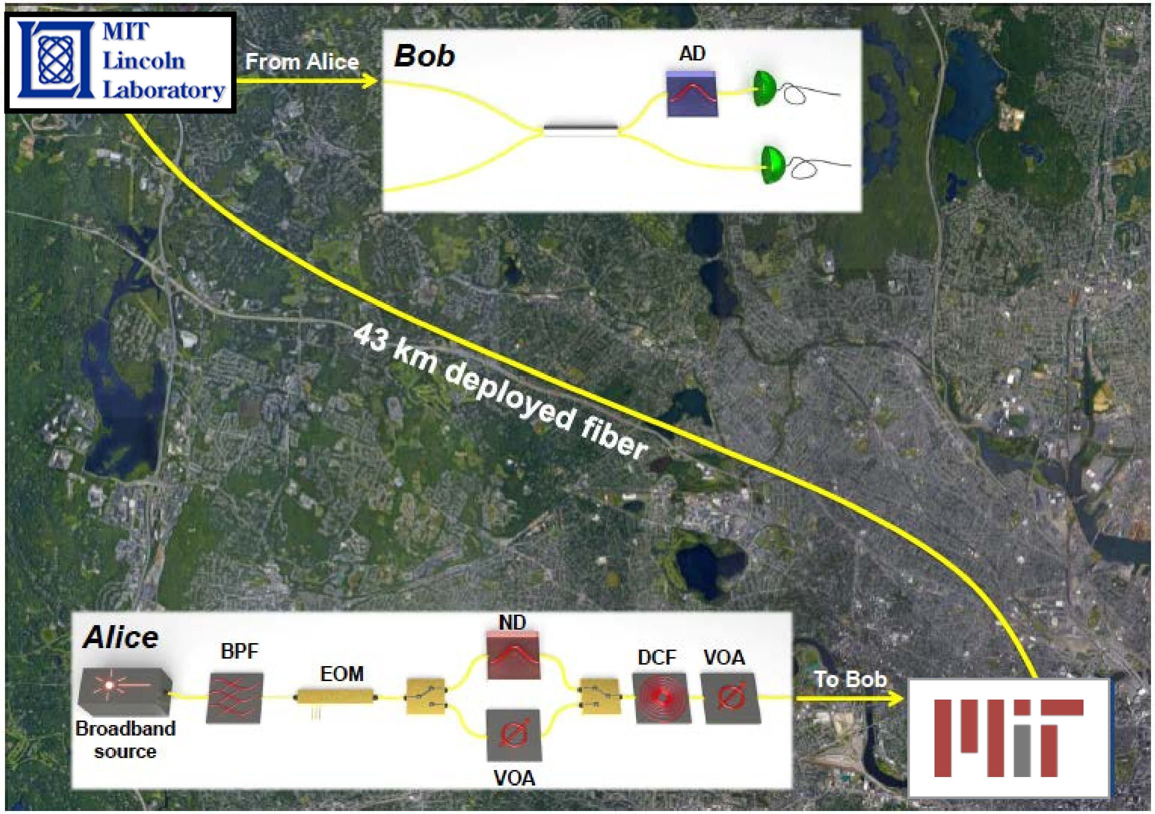
Assumptions:
- 10 GHz modulation rate
- 1 kHz background rate
- 93% detector efficiency
- 100 ns dead time after each detection event

High-dimensional QKD protocol

- Information per detected photon as much as $\log_2(M)$, M = photon time slots



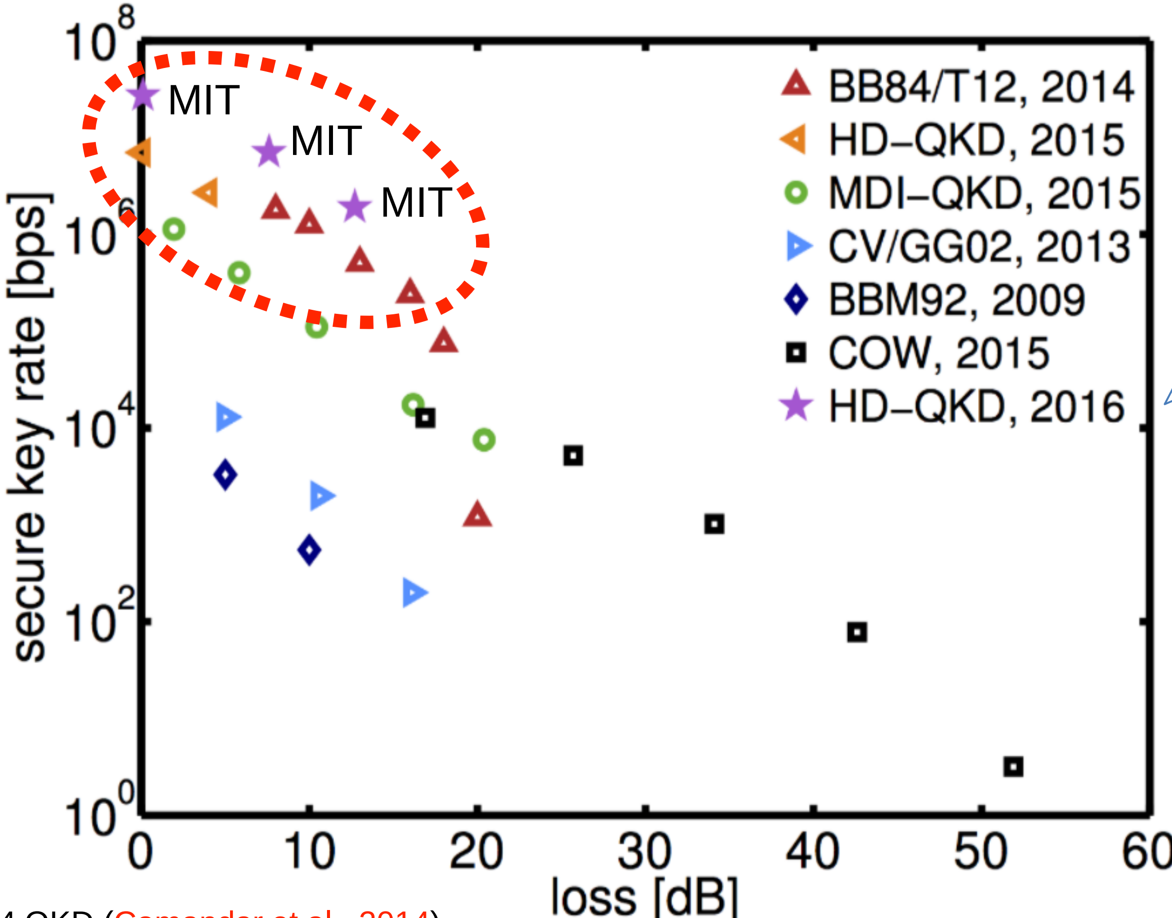
Boston-area quantum network testbed



	Back-to-back	41-km spool	43-km deployed fiber
Loss (dB)	0.1	7.6	12.7
Slot duration (ps)	240	240	240
Optimal M	16	8	4
Max. secret-key rate (bps)	23×10^6	5.3×10^6	1.2×10^6
Secure PIE (bit/photon)	1.40	0.88	0.50

Record rates!

Current QKD records



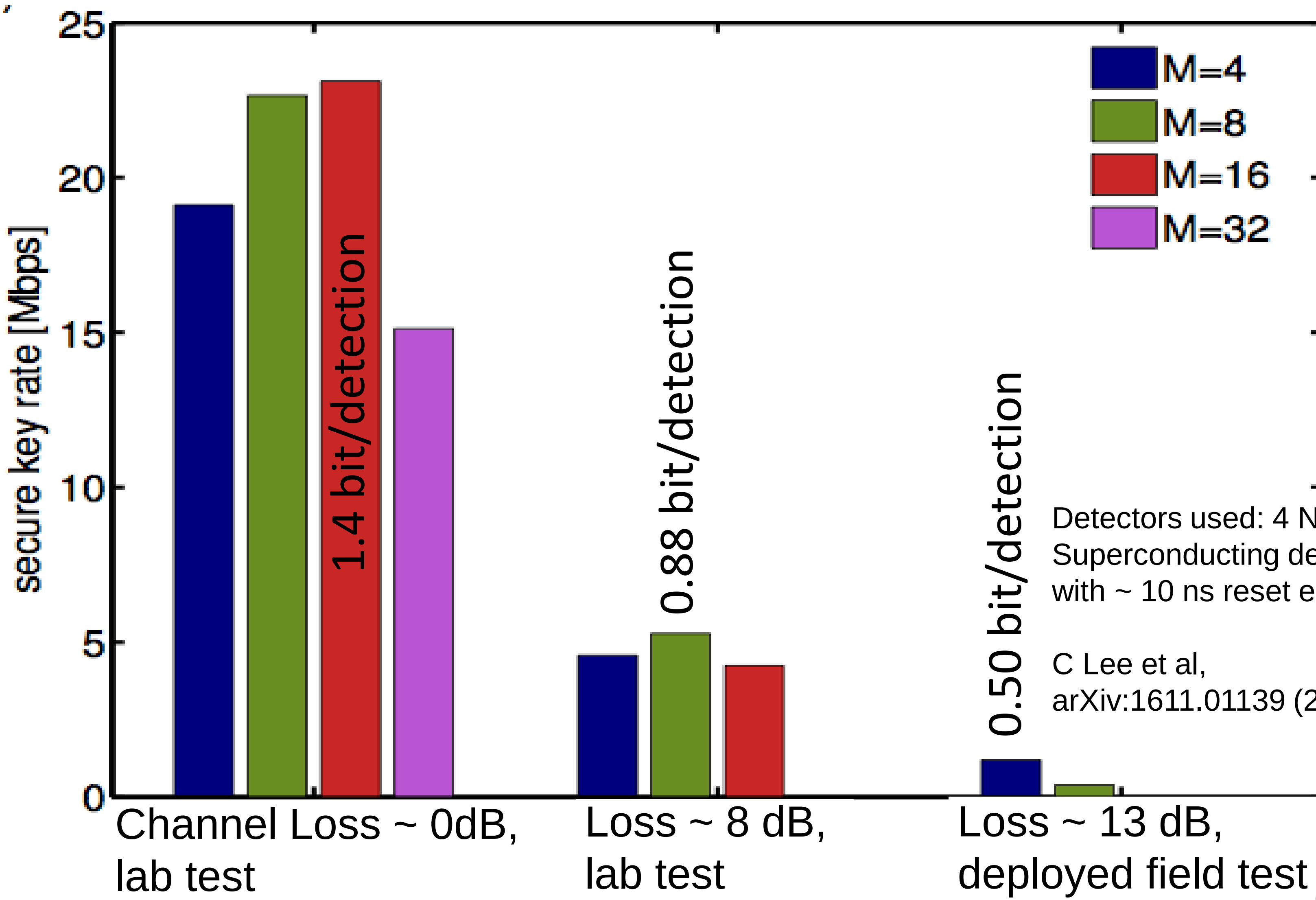
Decoy state, low-parity density check, privacy amplification, finite-key length

BB84 QKD (Comandar et al., 2014)
High-dimensional QKD (HD-QKD) (Zhong et al., 2015)
Measurement-device-independent QKD (MDI-QKD) (Comandar et al., 2016)

Continuous variable (CV)/GG02 QKD (Jouguet et al., 2013)
Six-state BBM92 QKD (Treiber et al., 2009)
Coherent-one-way (COW) QKD (Korzh et al., 2014)

The record highest secret key generation rate (HD-QKD, 2016) is our most recent experimental result (Lee et al., 2016).

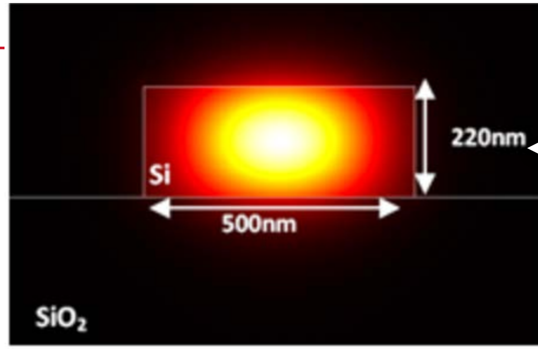
HD-QKD helps for moderate channel loss

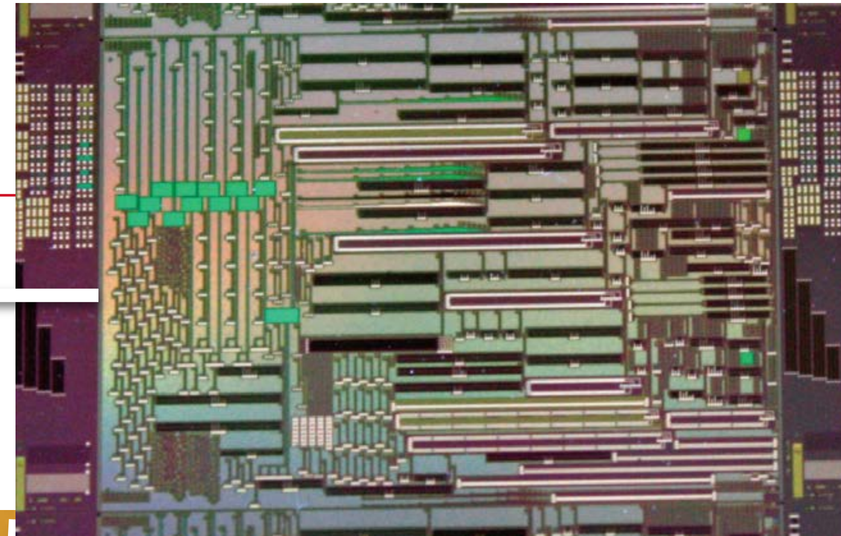


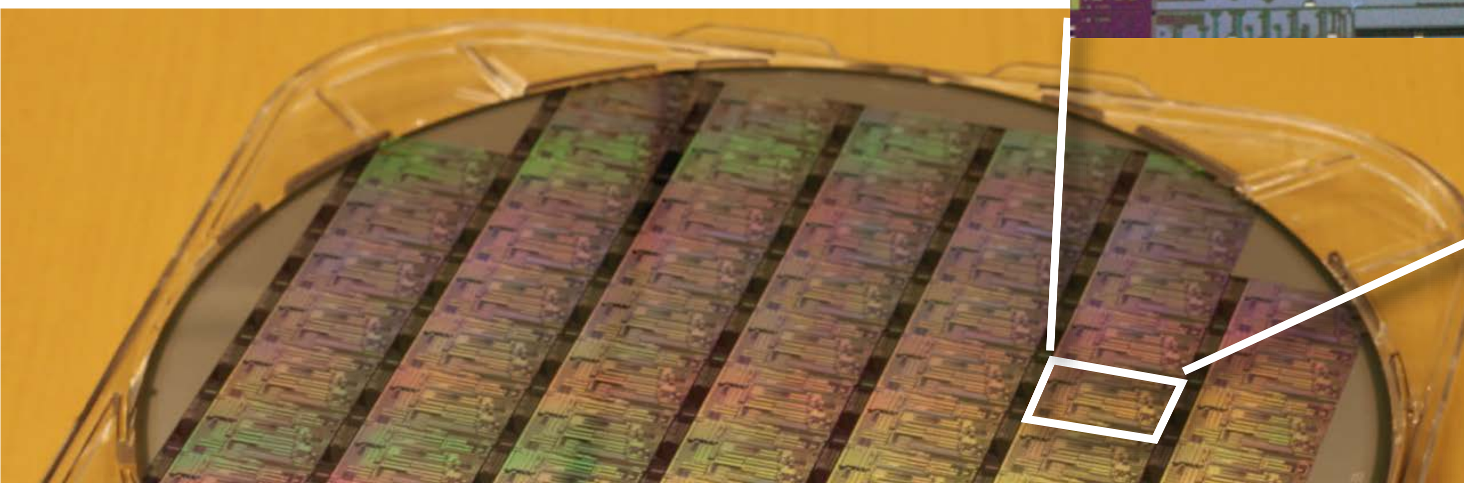
Detectors used: 4 NbN Superconducting detectors with ~ 10 ns reset each

C Lee et al, arXiv:1611.01139 (2016)

Silicon photonics for QKD







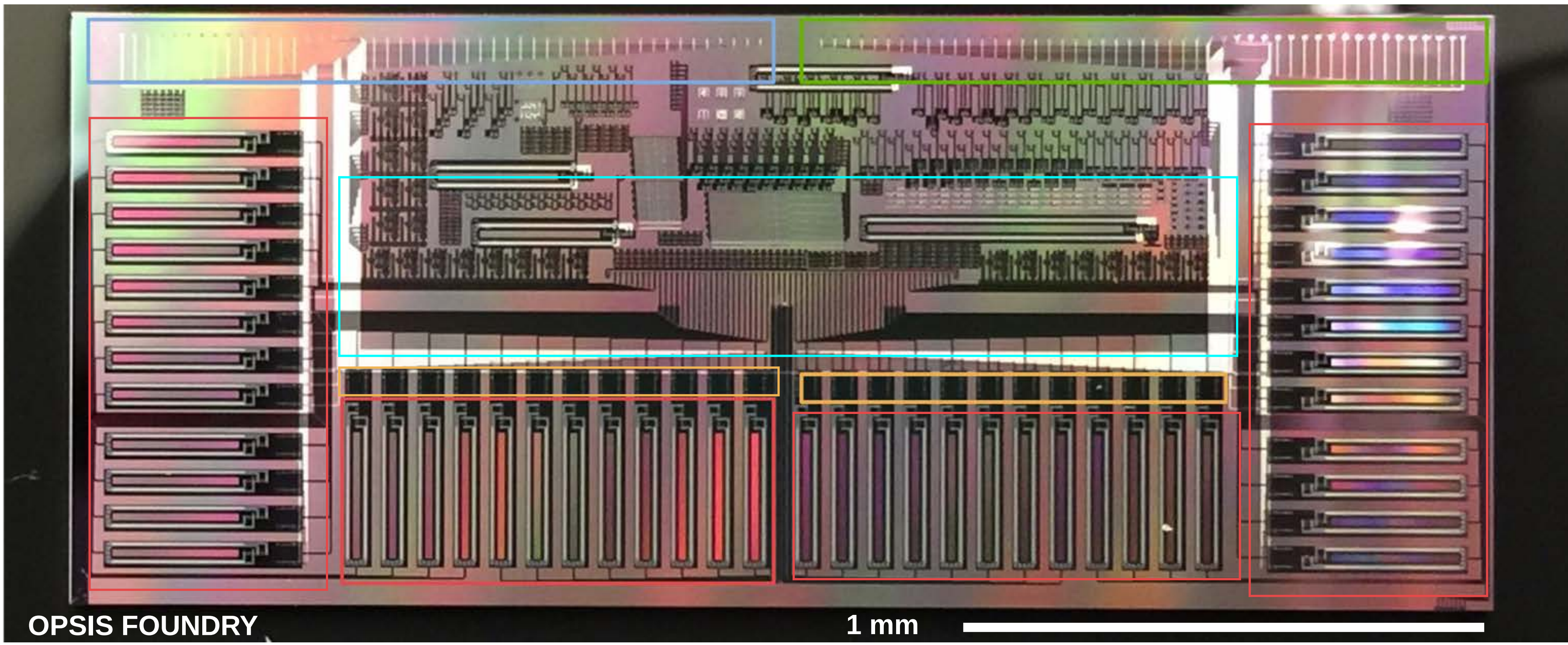
Switches: 1+GHz
Modulators: 10+ GHz
On-chip detectors: Ge and SNSPD
Interferometers: Contrast > 80dB (!)
Entangled photon sources (sFWM)
Dense Wavelength Division Multiplexing

QKD transmitters in Silicon Photonics:

- DWDM: 100x faster
- >100x cost reduction
- >10^3 volume reduction
- However, some modification needed

48-channel transmitter

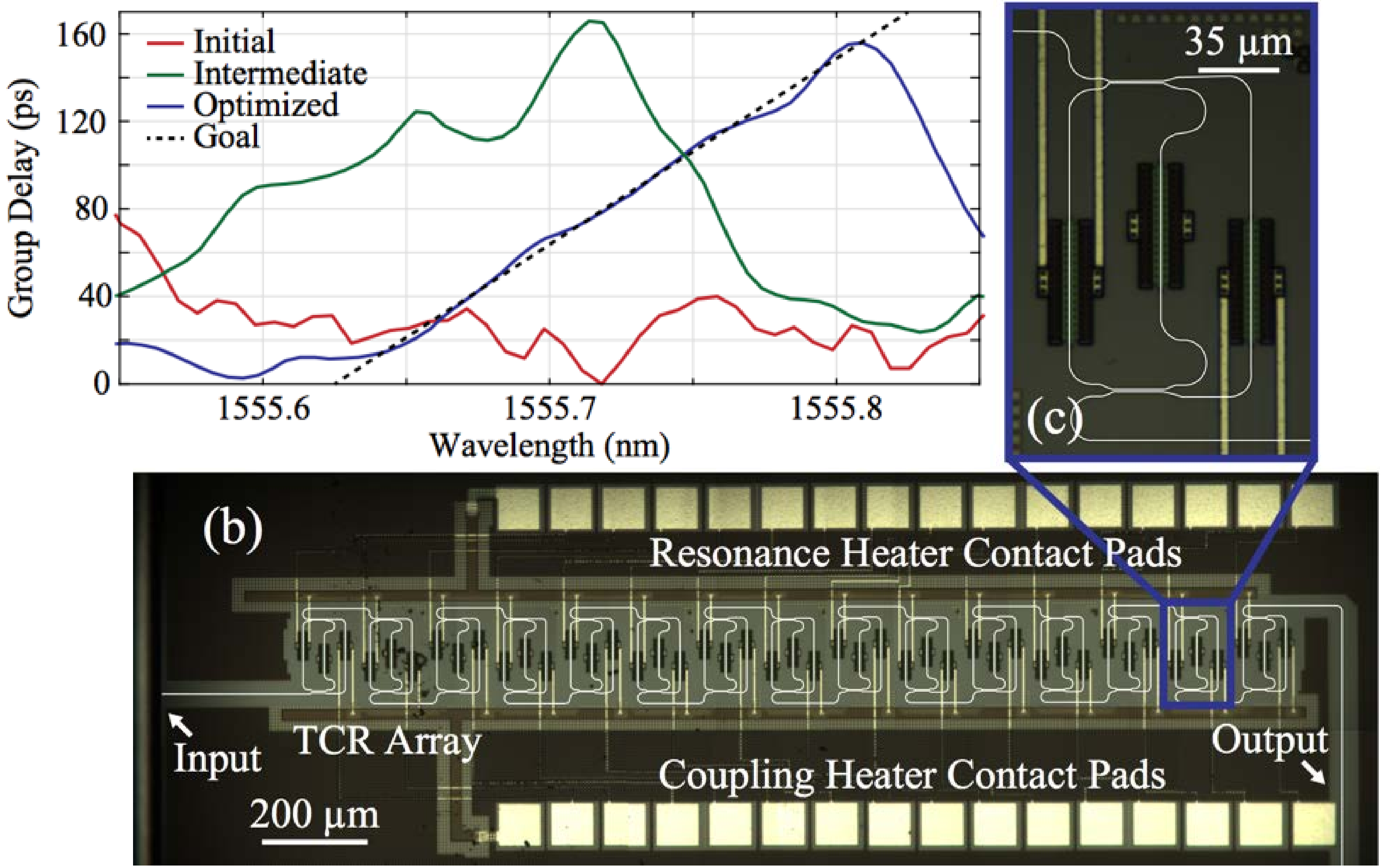
- Adapted from OpSIS foundry



48 Traveling Wave Modulators	Input Grating Couplers	Output Grating Couplers	Phase Modulators	Multiplex

With Michael Hochberg and Tom Baehr-Jones (Coriant)

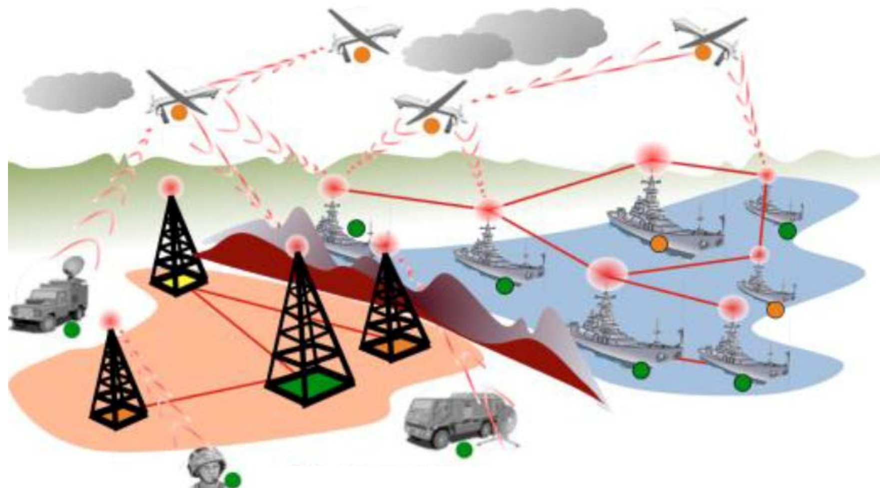
HD-QKD: PIC-tunable group velocity dispersion



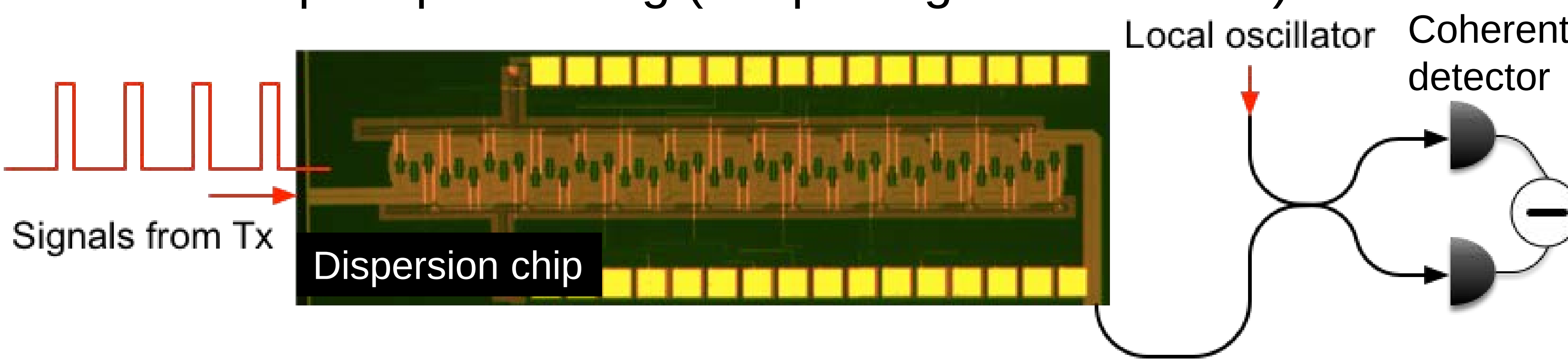
15 overcoupled ring filters with tunable quality factor and resonance frequencies

Additional uses of dispersion control

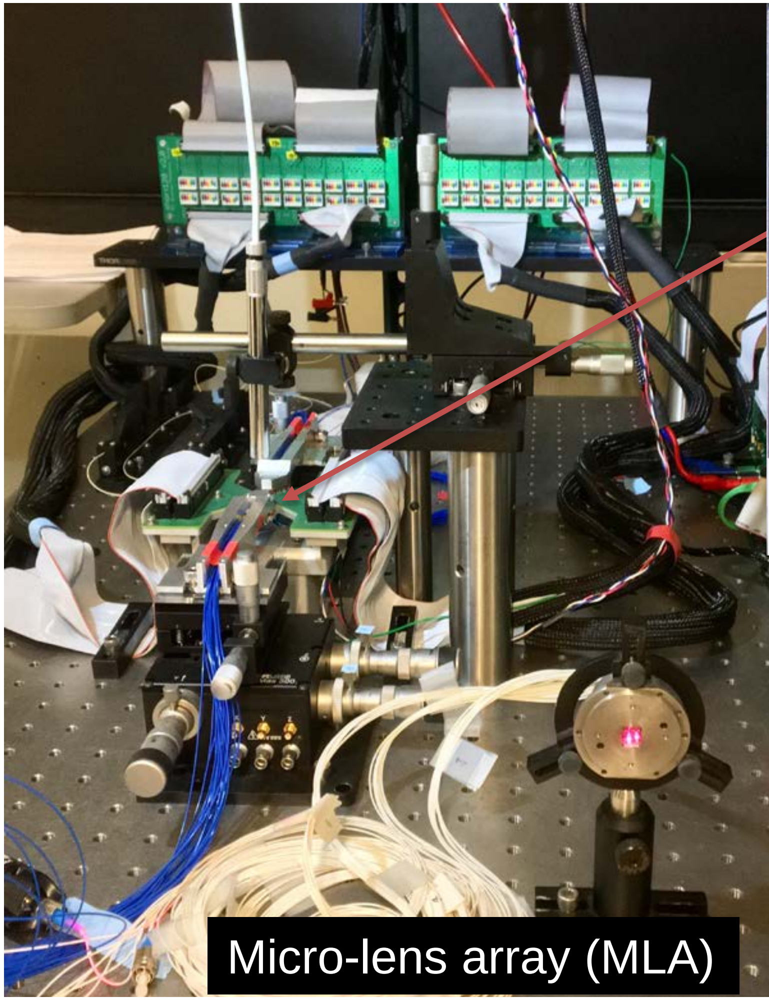
- Dynamic dispersion control for maritime applications

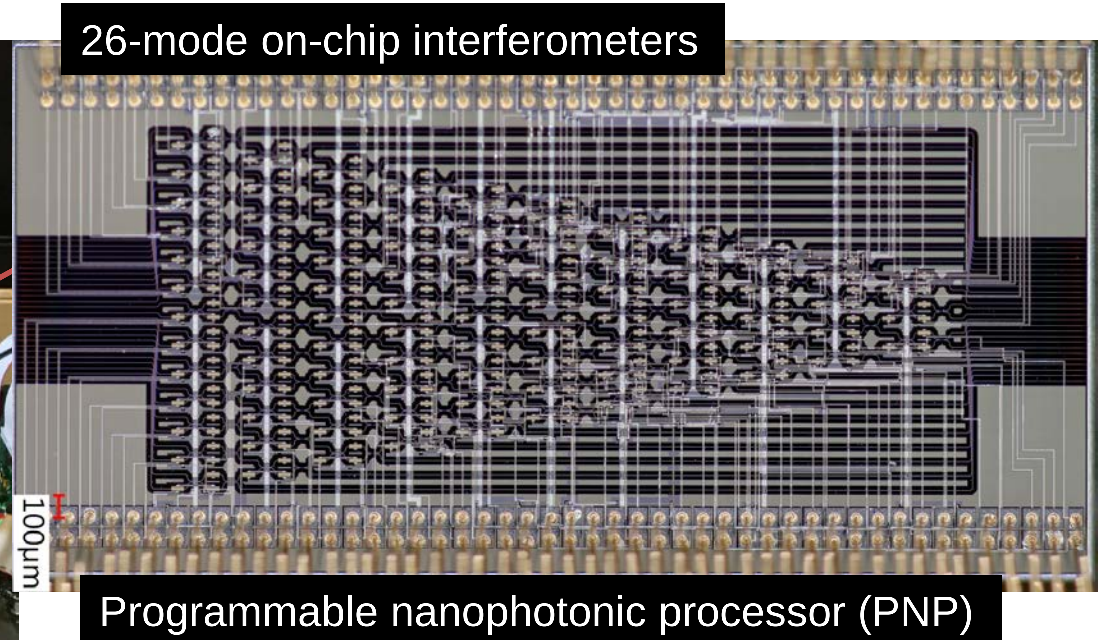


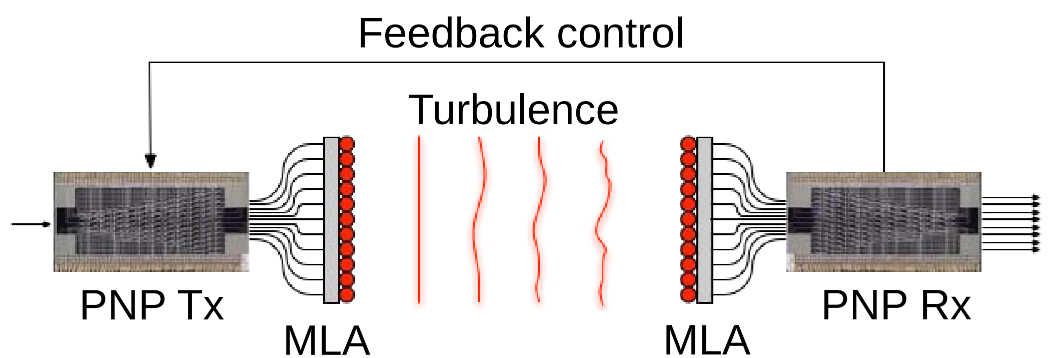
- Block post-processing (temporal green machine)



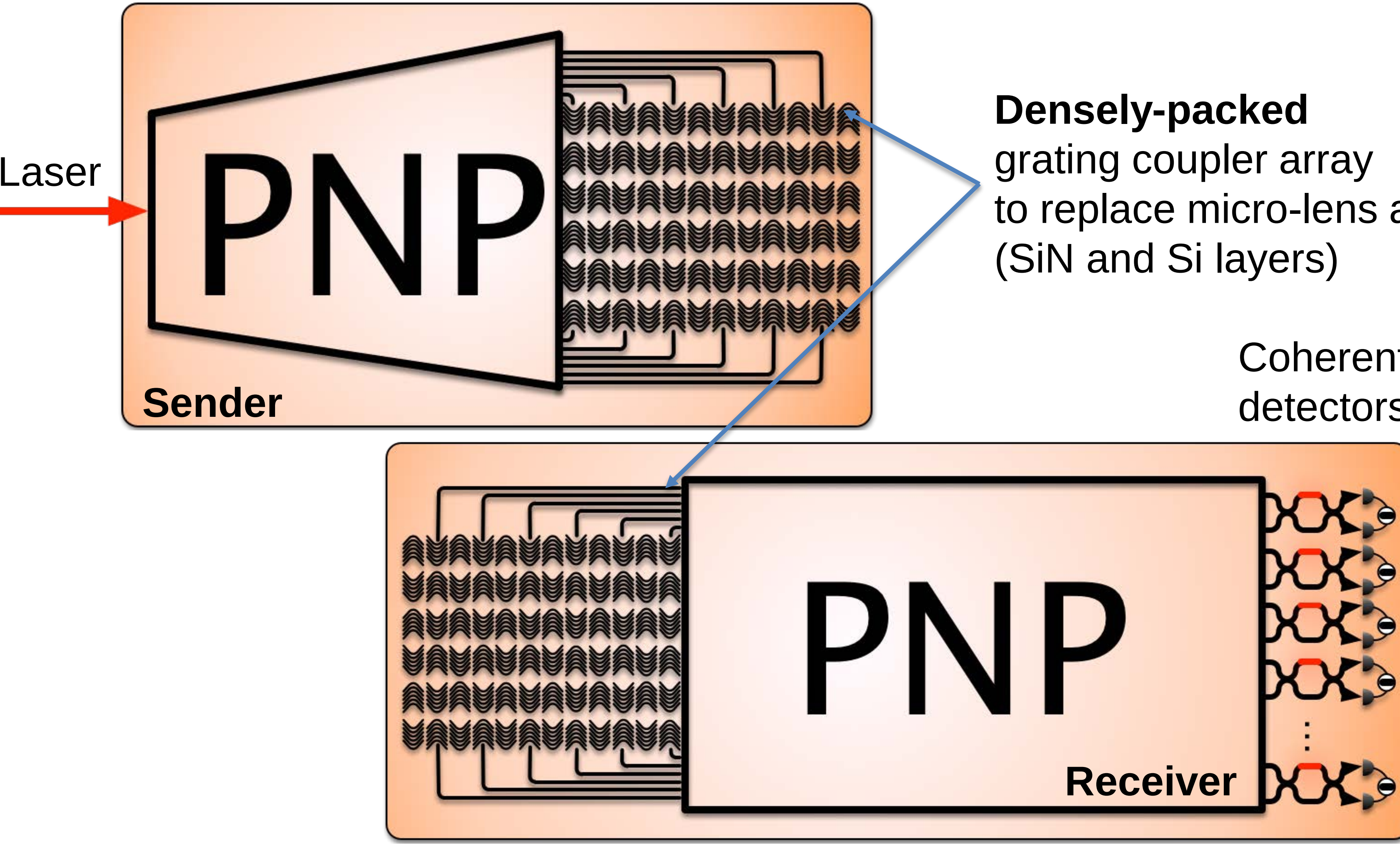
Adaptive transmitters and receivers







Programmable photonic integrated circuit

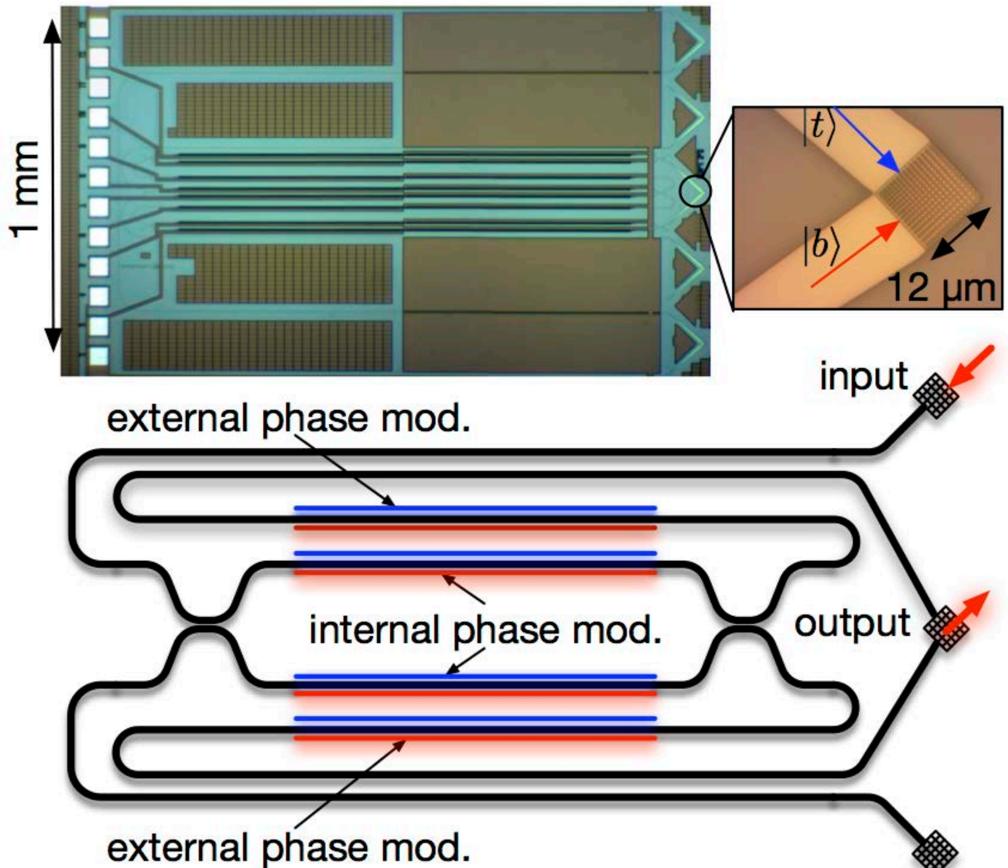


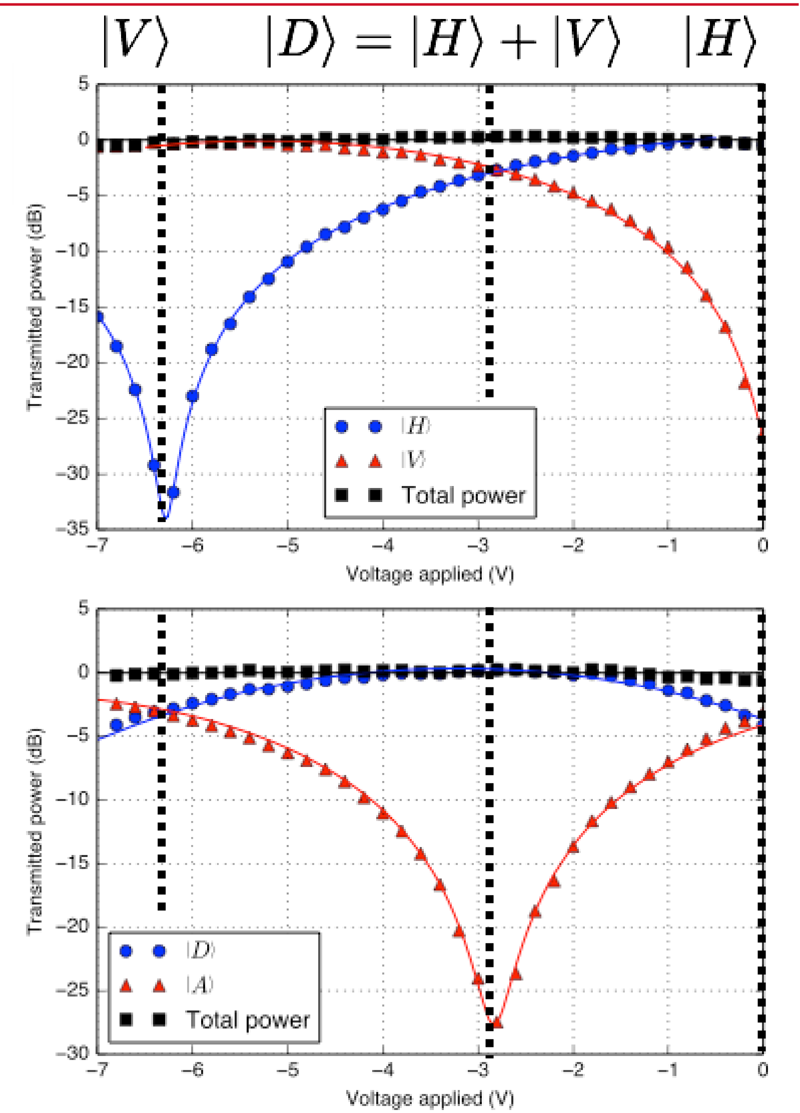
Densely-packed grating coupler array to replace micro-lens array. (SiN and Si layers)

Coherent detectors

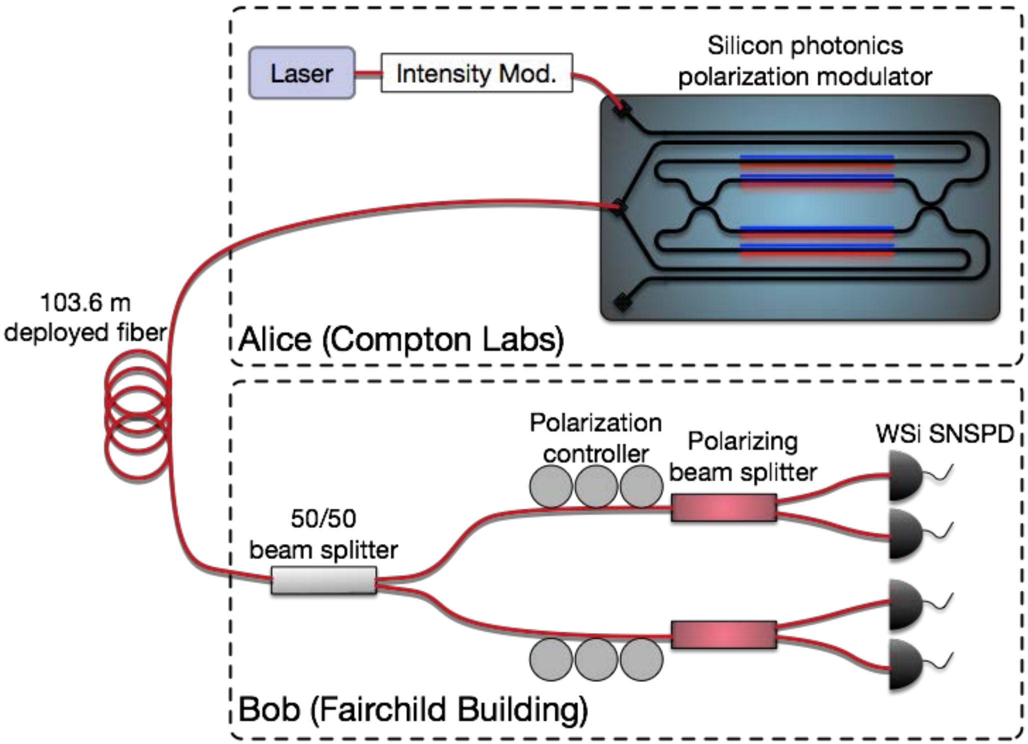
Polarization-based QKD

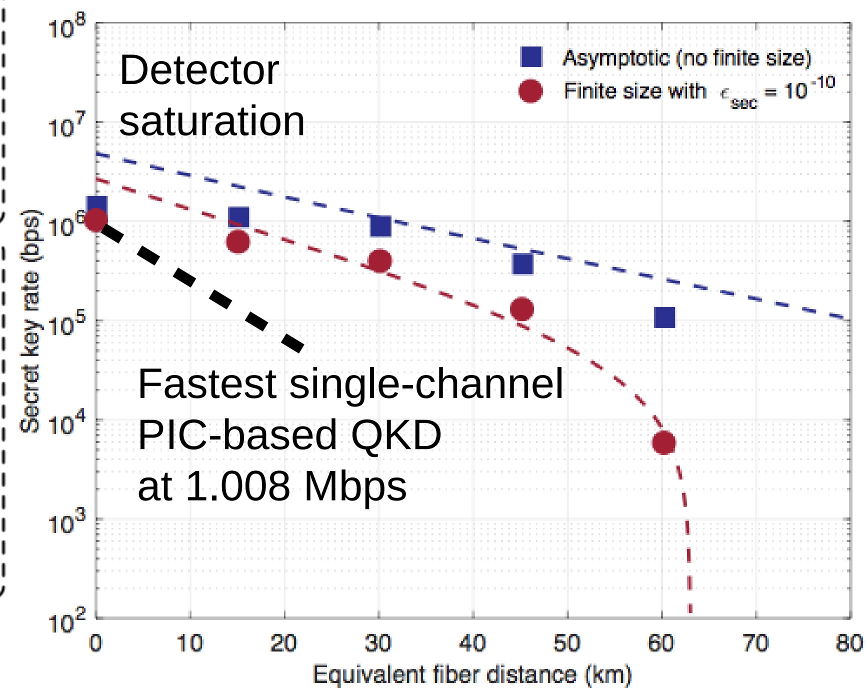
- BB84 protocol with polarization
- Polarization is robust against turbulence

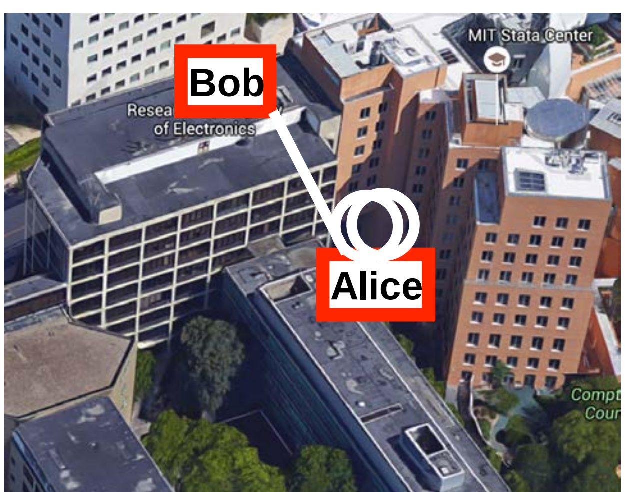




System performance in local field test







Summary

- Optimized secret-key capacity through HD-QKD
- Polarization-based QKD—resistant to turbulence
- Chip-based solutions for dispersion and adaptive control

	Adaptive control using PICs	Adaptive deformable mirrors
Size	Compact	Large
Configuration speed	~ 1 μs	~ 1 μs
Phase stability	Interferometers can be integrated	Needs phase stable interferometers
Degrees of freedom	Controls both phases & amplitudes	Controls only phases

Outlook

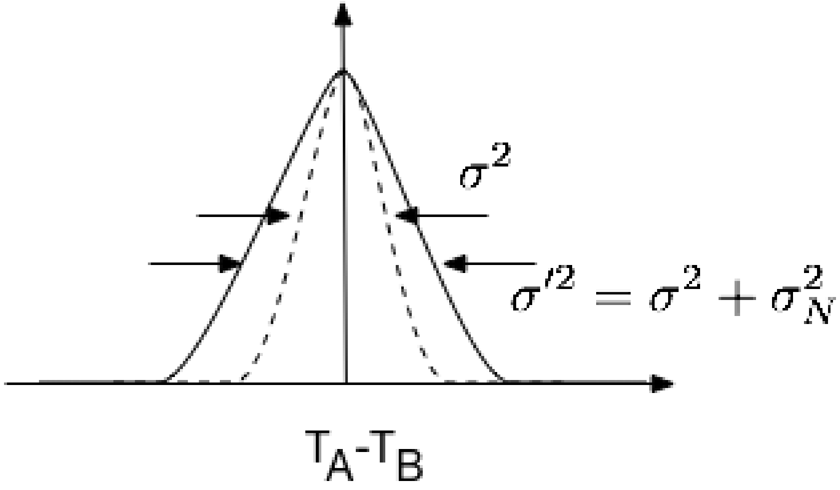
- Demonstration of QKD with 2-4 spectral channels
- Implementation of chip-based adaptive transmitter
- Demonstration of green machine

Appendix: Security of HD-QKD

$$\Delta I = \beta I(A;B) - \chi(A;E)$$

$$\Gamma' = \begin{pmatrix} \gamma'_{AA} & \gamma'_{AB} \\ \gamma'_{BA} & \gamma'_{BB} \end{pmatrix}$$

$$\gamma_{AB} = \frac{1}{2}\begin{pmatrix} \langle\{\hat{T}_A, \hat{T}_B\}\rangle & \langle\{\hat{T}_A, \hat{D}_B\}\rangle \\ \langle\{\hat{D}_A, \hat{T}_B\}\rangle & \langle\{\hat{D}_A, \hat{D}_B\}\rangle \end{pmatrix},$$



$$\gamma'_{AA} = \gamma_{AA},$$

$$\gamma'_{AB} = (\gamma'_{BA})^T = \begin{pmatrix} 1-\eta_t & 0 \\ 0 & 1-\eta_\omega \end{pmatrix}\gamma_{AB},$$

$$\gamma'_{BB} = \begin{pmatrix} 1-\epsilon_t & 0 \\ 0 & 1-\epsilon_\omega \end{pmatrix}\gamma_{BB}.$$

Saikat / Kathryn - team introduction, task descriptions, plan: **10 minutes**
Jeff - Security analysis w/ realistic eavesdropping assumptions: **15 minutes**
Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**
Kamil - security proof for discrete modulation CV QKD: **15 minutes**
Saikat - efficient post-processing for CV QKD: **15 minutes**
Mark - Finite key-length analysis for QKD: **15 minutes**
Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**
Saikat - Free-space quantum networking / wrap up - **15 minutes**

Communications and Networking with Quantum Operationally-Secure Technology for Maritime Deployment (CONQUEST)

Quantum networking

Saikat Guha
BBN

ONR CONQUEST Review
February 17, 2017

Raytheon BBN Technologies

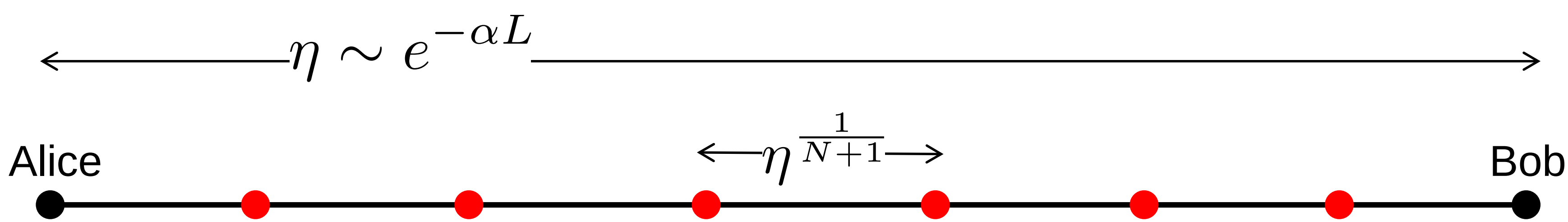
LSU Louisiana State University

rle at MIT Research Laboratory of Electronics at MIT

CipherQ

QKD over long distance

$$R_{\text{direct}}(\eta) = -\log(1-\eta) \approx 1.44\eta \text{ bits/mode}$$

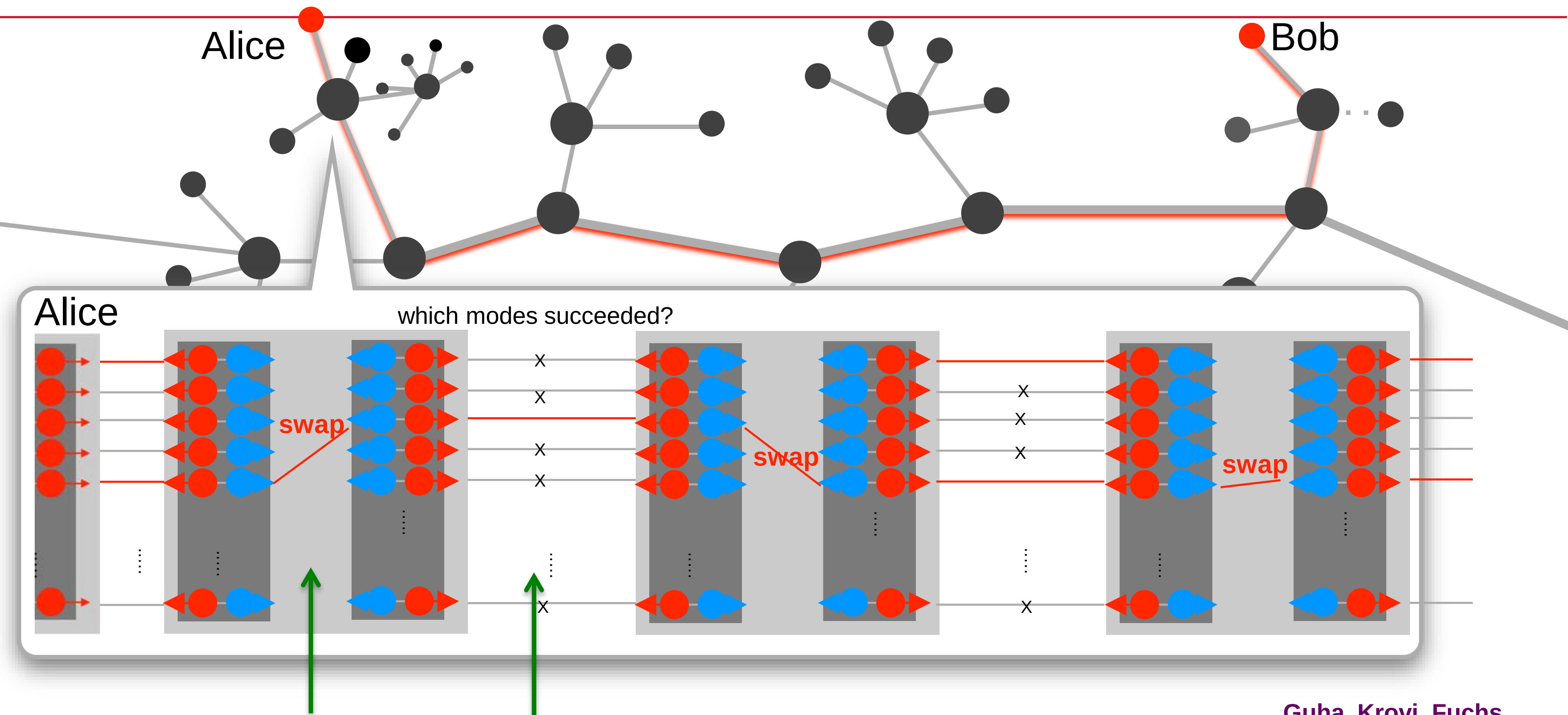


Repeaters: a special purpose quantum processor

$$R \leq \log\left[\frac{1}{1-\eta^{\frac{1}{N+1}}}\right] \approx \eta^{\frac{1}{N+1}}$$

– More repeater nodes is better if the repeater nodes are perfect
– What if repeater nodes are constructed out of lossy / imperfect devices? What does is take to outperform R_{direct}?

All-photonic quantum repeaters



q

Site

$$p = 1 - (1-p_0)^M$$ **Bond**

$$p_0 \propto \eta^{1/(N+1)}$$

$$R \sim p^{N+1} q^N$$

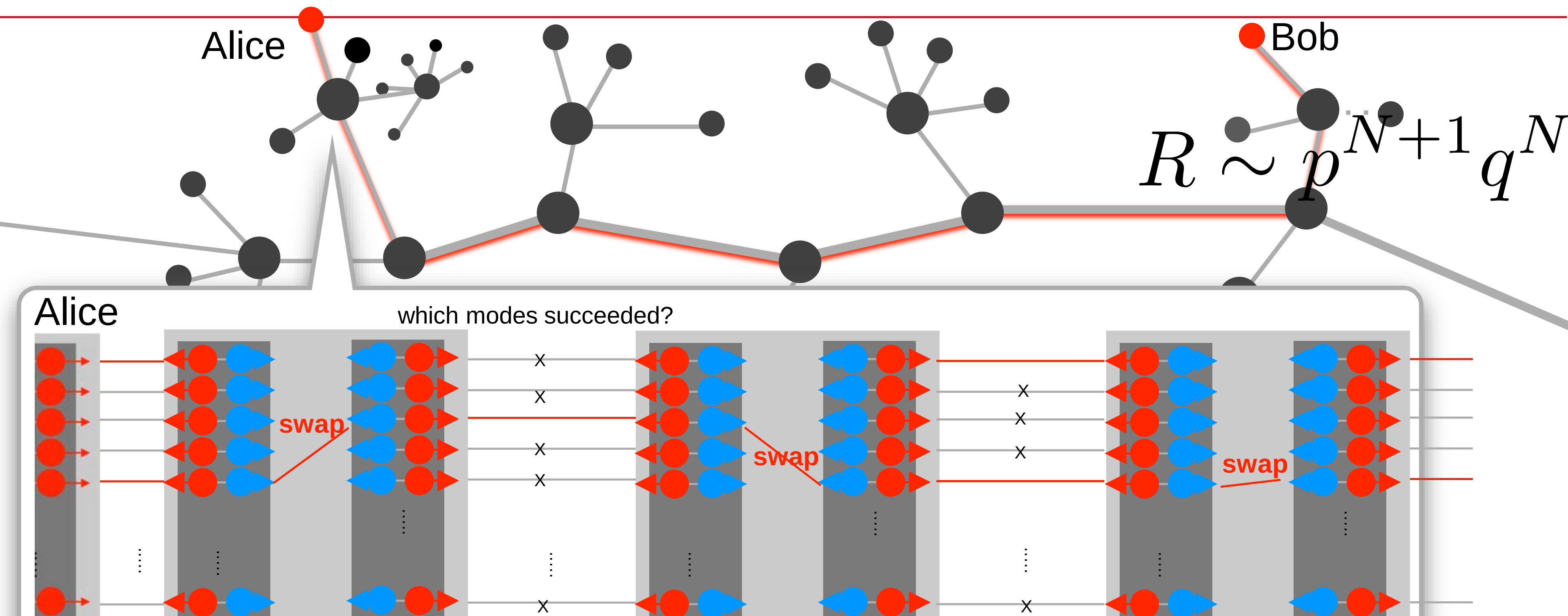
Guha, Krovi, Fuchs, Dutton, Simon, Tittel, PRA (2015)

Azuma, Tamaki, Lo, NCOMM (2015).

M Pant et al, PRA 95, No.1 (2017)

M Pant, H Krovi, D Englund, SG, PRA 95, No.1 (2017)

All-photonic quantum repeaters



$$R \sim p^{N+1} q^N$$

	matter qubits	photons
Quantum memory	cold atoms, atom-like, SC emitters	cluster states
Photonic interfaces	challenging	OK
Efficient ent't SWAP	soon	challenging
Wavelength	challenging	OK
Many qubits	10s of physical qubits (5-10 years)	challenging
Temperature	cold	*OK*

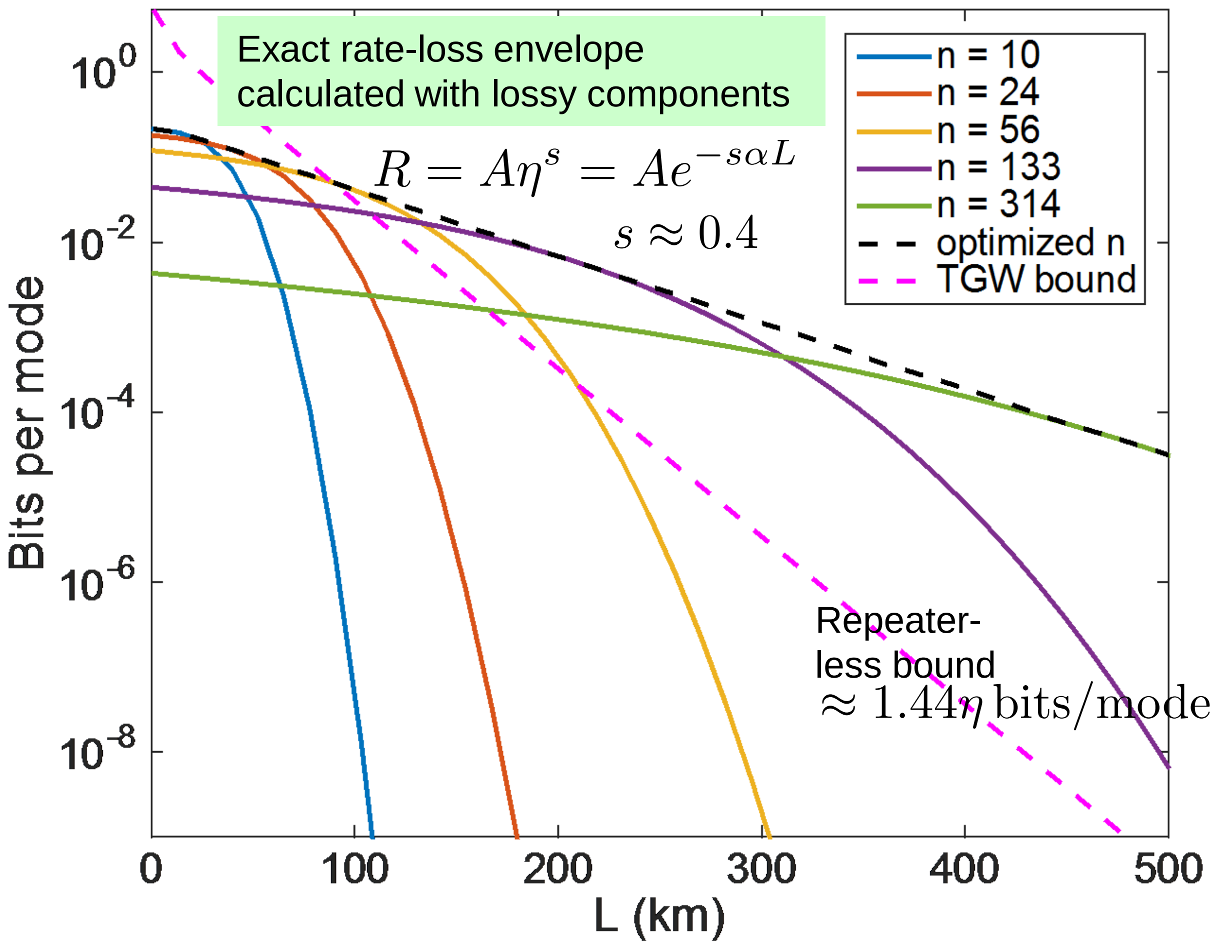
Guha, Krovi, Fuchs, Dutton, Simon, Tittel, PRA (2015)

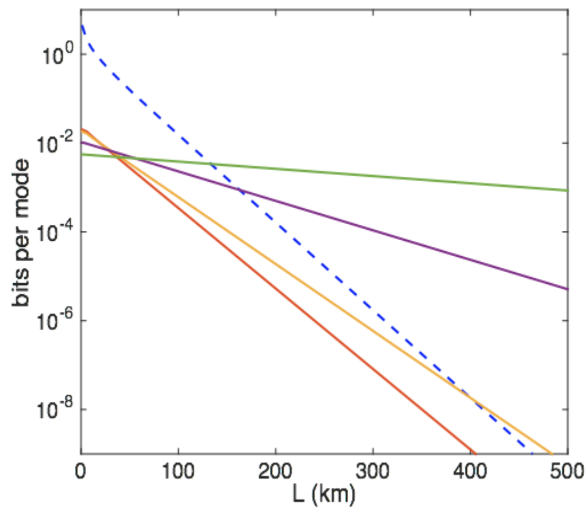
Azuma, Tamaki, Lo, NCOMM (2015).

M Pant et al, PRA 95, No.1 (2017)

M Pant, H Krovi, D Englund, SG, PRA 95, No.1 (2017)

All photonic quantum repeater: two-way, DV





Resources required to just beat repeaterless bound

3M SPS per node →

200K SPS per node →

15 K GHZ state sources per node

Azuma, Tamaki, Lo, Nature Communications 6, 6787 (2015)

Pant, Krovi, Englund, and SG, PRA 95, 012304 (2017)

All photonic quantum repeater: one-way, DV

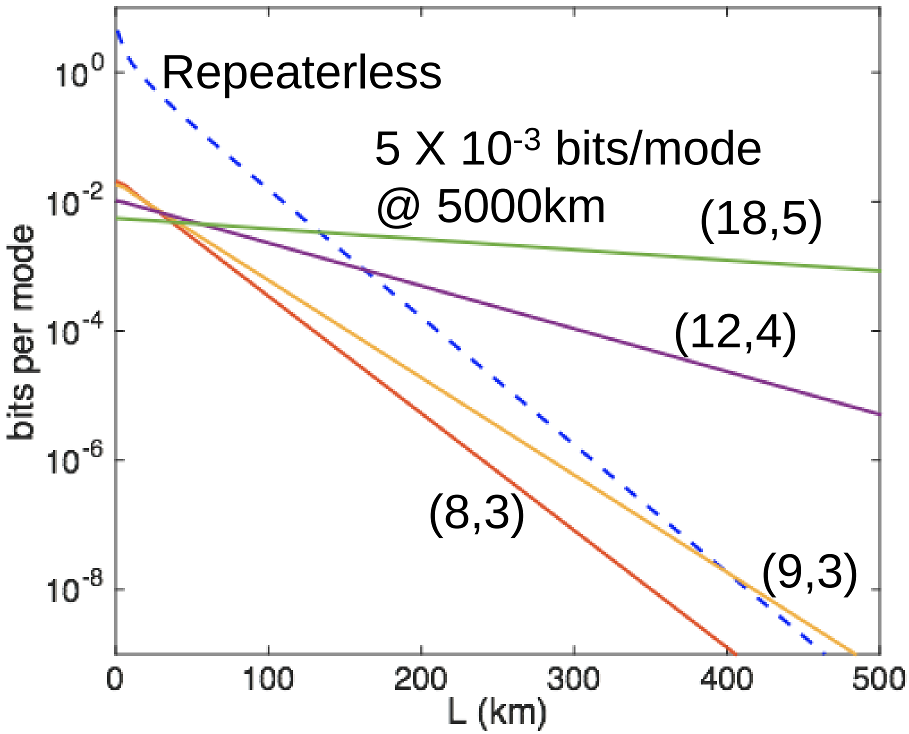
$$|\pm\rangle^{(n,m)} = \left(\frac{|0\rangle^{\otimes m} \pm |1\rangle^{\otimes m}}{\sqrt{2}}\right)^{\otimes n}$$

Quantum Parity Code

Bell measurement success probability = $1-1/2^n$

Ewert, F., Bergmann, M., & van Loock, P. PRL, 117 (21) 210501, 2016

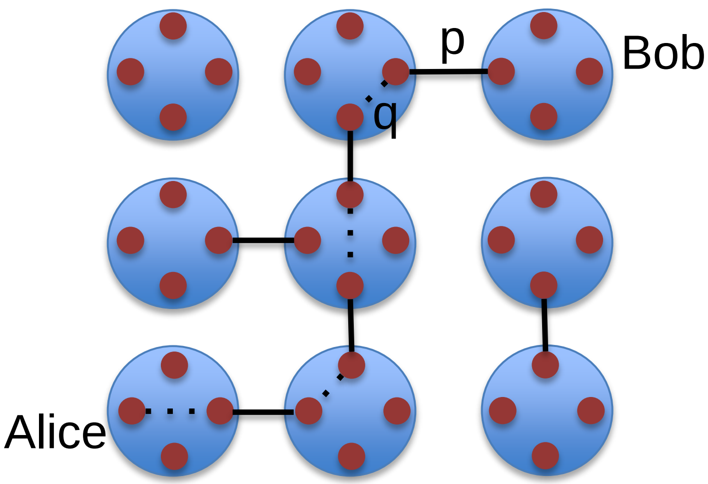
(m,n)	size of state	# of single-photon-sources	# 3-GHZ state sources
(8,3)	48	200k	1k
(9,3)	54	700k	3.5k
(12,4)	96	2M	10k
(18,5)	180	4.4M	22k

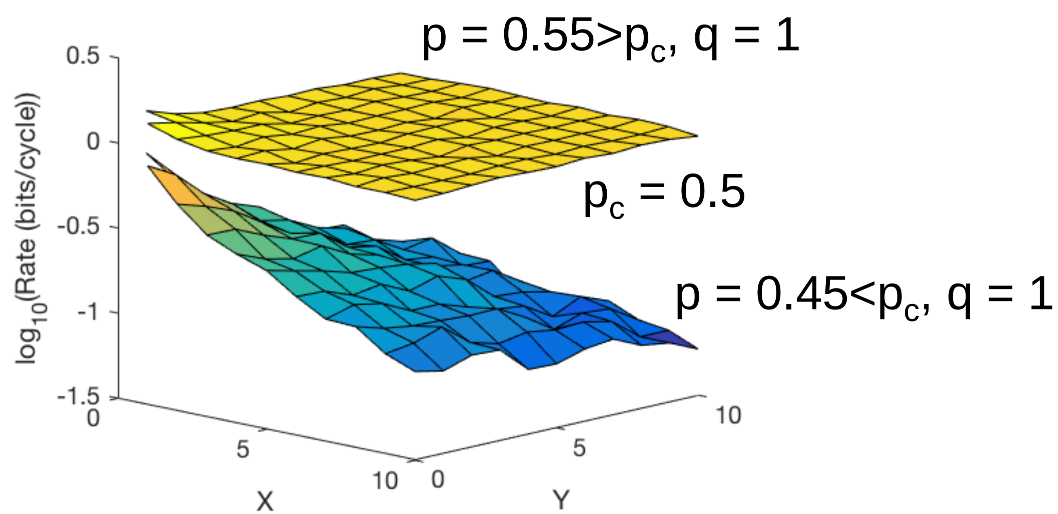


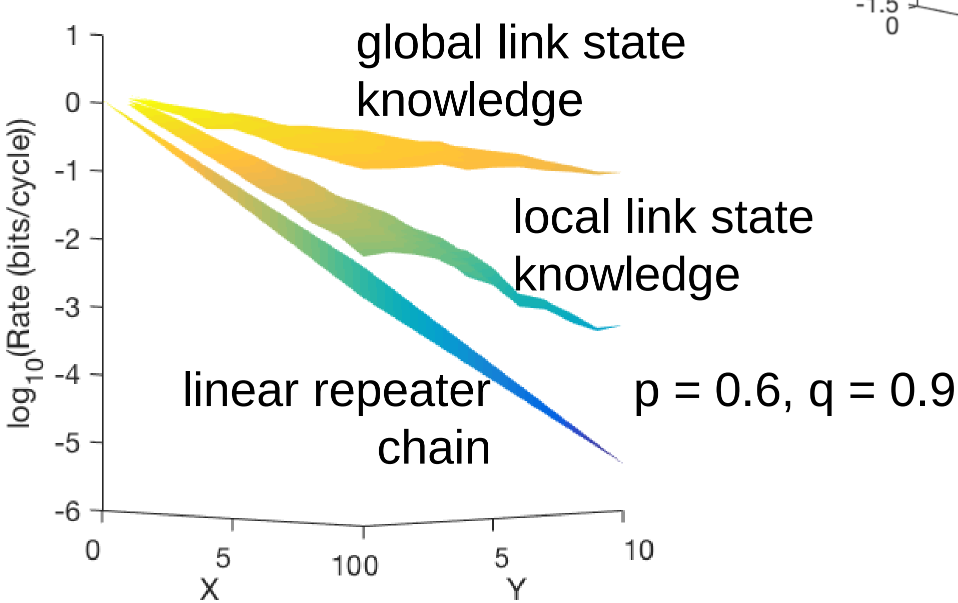
Device parameter	symbol	value
fiber loss coefficient	α	0.046 km^{-1} (0.2 dB/km)
on-chip loss coefficient	β	0.62 m^{-1} (2.7 dB/m)
feed-forward time in fiber	τ_f	102.85 ns
feed-forward time on-chip	τ_s	20 ps
chip to fiber coupling efficiency	P_c	0.99
source detector efficiency product	$\eta_s\eta_d$	0.99
speed of light in fiber	c_f	$2 \times 10^8 m/s$
speed of light on chip	c_{ch}	$7.6 \times 10^7 m/s$

M. Pant, S. Muralidharan, L. Jiang, D. Englund, and SG (in preparation, 2017)

Multipath routing in quantum repeater network





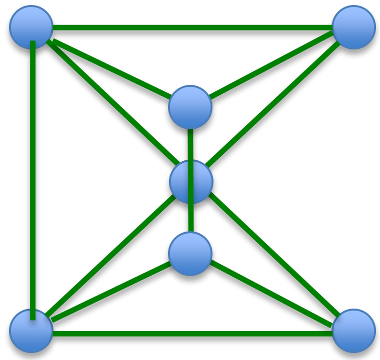


Even with only local information, 2D repeater networks outperform linear repeater chains

M. Pant, L. Jiang, D. Englund, D. Towsley, P. Basu, H. Krovi and SG (in preparation, 2017)

How should repeaters be placed?

- Euclidean Steiner Tree problem: NP hard
  - Minimize the total length of pipes connecting cities



Basu and Guha, work in progress, unpublished (2017)

- Repeater placement is a more complication version of the Euclidean Steiner Tree problem
  - Given user nodes (n potential Alice-Bob pairs), and proportional rate requirements for each of the n flows, and given optimal routing protocols at each repeater node (ideally assuming local link-state knowledge), and physical resource constraints (e.g., sources, detectors), what number / placement of repeaters is maximizes rate?

Repeater for CV QKD?

- Amplifiers (even phase-sensitive, quantum noise limited) do not help as quantum repeaters

Namiki, Gittsovich, Guha, Lutkenhaus, Phys. Rev. A (2014)

- No concrete notion of repeater known for CV QKD that beats repeater less rate bound
- Non-deterministic linear amplifiers: suggested by Tim Ralph – NOT clear if it can beat R_{direct}
- Alternative repeater techniques for CV. Developing CV / hybrid error correction techniques

CONQUEST program

- Task 1: QKD operation and security analysis for a naval atmospheric link with a realistic eavesdropper
- Task 2: Maritime-implementable QKD protocols
- Task 3: Maximizing the information efficiency of QKD
- Task 4: Improved hardware-domain signal processing
- Task 5: QKD network via un-trusted quantum nodes
- Task 6: Important technical issues to address current deficiencies in the theory/practice of QKD

Saikat / Kathryn - team introduction, task descriptions and technical plan: **10 minutes**

Jeff - Security analysis with realistic eavesdropping assumptions: **15 minutes**

Jeff / Franco - Flood light QKD: theory and experiments: **15 minutes**

Kamil - security proof for discrete modulation CV QKD: **15 minutes**

Saikat - efficient post-processing for CV QKD: **15 minutes**

Mark - Finite key-length analysis for QKD: **15 minutes**

Darius / Dirk - PIC based transmitters and receivers for QKD: **15 minutes**

Saikat - Free-space quantum networking / wrap up - **15 minutes**